KESSLER TOPAZ
MELTZER & CHECK, LLP
Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

KESSLER TOPAZ
MELTZER & CHECK, LLP
Joseph H. Meltzer
jmeltzer@ktmc.com
Melissa L. Yeates
myeates@ktmc.com
Tyler S. Graden
tgraden@ktmc.com
Jordan E. Jacobson
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiff and the proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

JOHN DOE, Individually and on behalf of all others similarly situated,

Plaintiff,

v.

KAISER FOUNDATION HEALTH PLAN, INC., KAISER FOUNDATION HOSPITALS, and THE PERMANENTE MEDICAL GROUP, INC.

Defendant.

Case No. 4:23-cv-02207

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

TABLE OF CONTENTS

Plaintiff[1] brings this proposed class action against Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical Group, Inc. (collectively "Kaiser Permanente" or "Defendants"), individually and on behalf of all others similarly situated, upon personal knowledge as to Plaintiff's own conduct, and on information and belief as to all other matters based on investigation by counsel.[2]

I. NATURE OF THE ACTION

1. As any reasonable patient would expect, Plaintiff trusted that his medical providers would treat the information that he shared with them as private and confidential.

2. This expectation extends to Plaintiff's use of Kaiser Permanente's websites, on which he and other patients would schedule appointments, access medical test results, learn about treatment options, exchange messages and healthcare information with providers, participate in online health assessments, pay bills, and research specialists, among other sensitive activities.

3. Notwithstanding, Plaintiff and other patients' reasonable expectation that their interactions and communications through Kaiser Permanente's website would not be shared with third parties, Kaiser Permanente discloses the contents of patients' confidential information and communications with a number of third parties, completely unbeknownst to Plaintiff and its other patients, while those communications are in transit between Plaintiff and Class Members on the one hand and Kaiser Permanente on the other.

4. Specifically, unbeknownst to Plaintiff and its other patients, Kaiser Permanente has installed code from multiple third parties throughout the Kaiser Permanente website that allows third party companies such as Quantum Metric, Twitter, Adobe, Bing, and Google (collectively, "Third

[1] Plaintiff seeks to proceed anonymously, as other plaintiffs have in other litigation claiming privacy violations involving health care providers. *See, e.g.*, Class Action Complaint & Demand for Jury Trial, *Doe. v. Meta Platforms Inc., Inc.*, No. 22-cv-3580 (N.D. Cal. June 17, 2022), ECF No. 1; Class Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*, No. 22-cv-04680 (N.D. Cal. Aug. 15, 2022), ECF No. 1; Complaint, *Doe v. Meta Platforms Inc.*, No. 22-cv-4963 (N.D. Cal. Aug. 30, 2022), ECF No. 1; Class Action Complaint & Demand for Jury Trial, *Doe v. Meta Platforms Inc.*, No. 22-cv-6665 (N.D. Cal. Oct. 28, 2022), ECF No. 1; Complaint, *Doe v. Meta Platforms Inc.*, No. 22-cv-4293 (N.D. Cal. July 25, 2022), ECF No. 1. Plaintiff will seek Defendants' consent to proceed anonymously.

[2] Counsel's investigation includes an analysis of publicly available information. Plaintiff believes that a reasonable opportunity for discovery will provide further support for the claims alleged herein.

Party Wiretappers") to intercept the content of Plaintiff and Class Members' patient status, identifying information, medical topics researched, choices made, information shared and communications with their medical providers, including personally identifiable medical information and other confidential information and communications, when that information is in transit.

5. The third party code that Kaiser Permanente has installed on its website transmits and redirects the content of Plaintiff and other Class Members' communications to these Third Party Wiretappers from the very moment that a user first loads Kaiser Permanente's website and continues as the user navigates through the website researching and sharing sensitive information.

6. Once the website loads, the Third Party Wiretappers continue to intercept the content of patients' communications with Kaiser Permanente in real time as the patient navigates the website to access specific medical information, clicks buttons that divulge sensitive and protected patient status, and personal and health information, and enters information into various fields on Kaiser Permanente's website, such as: (1) signing-up for a patient Portal; (2) signing-in or signing-out of a patient portal; (3) taking actions inside a patient Portal; (4) making, scheduling, or participating in appointments; (5) exchanging communications relating to doctors, treatments, payment information, health insurance information, prescription drugs, prescriptions, side effects, conditions, diagnoses, prognoses, or symptoms of health conditions; and (6) providing other information that qualifies as "personal health information" and/or identifying information under federal and state laws.

7. Kaiser Permanente knew that by embedding the Third Party Wiretappers' code, they were disclosing and permitting these Third Party Wiretappers to intercept and collect information shared by its website users, including the content of Plaintiff and Class Members' communications, which include identifying information, personal and sensitive information relating to medical treatment, and/or information that Kaiser Permanente was required to protect under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. § 1320d-6.

8. In fact, in December 2022, the United States Department of Health and Human Services ("HHS") issued a bulletin "to highlight the obligations" of health care providers under the HIPAA Privacy Rule "when using online tracking technologies" such as those used by Kaiser

Permanente which "collect and analyze information about how internet users are interacting with a regulated entity's website or mobile application."[3]

9. In the bulletin, HHS confirmed that HIPAA applies to health care providers' use of tracking technologies like those developed by the Third Party Wiretappers and used by Kaiser Permanente. Among other things, HHS explained that health care providers violate HIPAA when they use tracking technologies that disclose an individual's identifying information even if no treatment information is included and even if the individual does not have a relationship with the health care provider:

> How do the HIPAA Rules apply to regulated entities' use of tracking technologies?
>
> Regulated entities disclose a variety of information to tracking technology vendors through tracking technologies placed on a regulated entity's website or mobile app, including individually identifiable health information (IIHI) that the individual provides when they use regulated entities' websites or mobile apps. This information might include an individual's medical record number, home or email address, or dates of appointments, as well as an individual's IP address or geographic location, medical device IDs, or any unique identifying code. **All such IIHI collected on a regulated entity's website or mobile app generally is PHI, even if the individual does not have an existing relationship with the regulated entity and even if the IIHI, such as IP address or geographic location, does not include specific treatment or billing information like dates and types of health care services**. This is because, when a regulated entity collects the individual's IIHI through its website or mobile app, the information connects the individual to the regulated entity (*i.e.*, it is indicative that the individual has received or will receive health care services or benefits from the covered entity), and thus relates to the individual's past, present, or future health or health care or payment for care.

10. HHS further clarified that HIPAA applies to health care providers' webpages with tracking technologies even on webpages that do not require patients to login:

> Tracking on unauthenticated webpages
>
> . . . [T]racking technologies on unauthenticated webpages may have access to PHI, in which case the HIPAA Rules apply to the regulated entities' use of tracking technologies and disclosures to the tracking technology vendors. Examples of unauthenticated webpages where the HIPAA Rules apply include: The login page of a regulated entity's patient portal (which may be the website's homepage or a separate, dedicated login page), or a user registration webpage where an individual creates a login for the patient portal . . . [and pages] that address[] specific

[3] Press Release, *HHS Office of Civil Rights Issue Bulletin on Requirements under HIPAA for Online Tracking Technologies to Protect the Privacy and Security of Health Information*, HHS (Dec. 1, 2022), https://www.hhs.gov/about/news/2022/12/01/hhs-office-for-civil-rights-issues-bulletin-on-requirements-under-hipaa-for-online-tracking-technologies.html; *Use of Online Tracking Technologies by HIPAA Covered Entities and Business* Associates, HHS (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html.

> symptoms or health conditions, such as pregnancy or miscarriage, or that permits individuals to search for doctors or schedule appointments without entering credentials may have access to PHI in certain circumstances. **For example, tracking technologies could collect an individual's email address and/or IP address when the individual visits a regulated entity's webpage to search for available appointments with a health care provider.** In this example, the regulated entity is disclosing PHI to the tracking technology vendor, and thus the HIPAA Rules apply.

11. This HHS bulletin did not create any new obligations, but instead highlights obligations that have been in place for decades, with which Kaiser Permanente should have been complying.

12. Kaiser Permanente's disclosure of patients' patient status, identifying information and personal and sensitive heath information to the Third Party Wiretappers, including without adequate disclosure of its conduct to Plaintiff and Class Members, constitutes an egregious invasion of Plaintiff and Class Members' privacy and violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*; Cal. Const. art. I, § 1, and HIPAA, and constitutes intrusion upon seclusion and breach of Kaiser Permanente's express and implied promises and duties to its patients, including Plaintiff and members of the Classes.

II. THE PARTIES

A. Plaintiff

13. Plaintiff John Doe is a citizen of California, and resides in Camarillo, California.

14. Plaintiff is a Kaiser Foundation Health Plan member and has received medical treatment through Kaiser Foundation Hospitals and/or the Permanente Medical Group since 2010.

15. Plaintiff regularly uses Kaiser Permanente's website and Patient Portal to access medical information and communicate with his health care providers, including making appointments, researching providers and medical conditions, checking medical results, and reviewing his medical history.

16. Without Plaintiff's knowledge or consent, Kaiser Permanente allowed the Third Party Wiretappers to intercept, collect, read, attempt to read, and/or learn the contents or meaning of the contents of Plaintiff's patient status, identifying information, personal and sensitive health

information, and confidential communications with his health care providers through Kaiser Permanente's website while that information and those messages, reports, and/or communications were in transit.

B. Defendants

17. Defendant Kaiser Foundation Health Plan, Inc. is a health care provider headquartered in Oakland, California.

18. Kaiser Foundation Health Plan, Inc. has an integrated care model, offering both hospital and physician care through a network of hospitals and physician practices operating under the Kaiser Permanente name. Members of Kaiser Permanente health plans have access to hospitals and hundreds of other health care facilities operated by Kaiser Foundation Hospitals and Permanente Medical Groups across the United States.

19. Kaiser Foundation Health Plan, Inc. is financially responsible for the payment of medical services provided to its enrollees ("Kaiser Plan Members") or has accepted such financial responsibility under contract with one or more of the Kaiser Permanente entities. Kaiser Foundation Health Plan, Inc. is the largest health care service plan in the United States, with over 11.8 million members in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, and Washington) and the District of Columbia.

20. Kaiser Foundation Hospitals is a non-profit, public-benefit corporation headquartered in Oakland, California. Kaiser Foundation Hospitals operates nearly 40 acute care hospitals and 680 medical offices in eight states (California, Colorado, Georgia, Hawaii, Maryland, Oregon, Virginia, and Washington) and Washington D.C., with its largest presence being in California, where the majority of its hospitals are located. Kaiser Foundation Hospitals employs more than 21,000 physicians, representing all medical fields.

21. The Permanente Medical Group, Inc. is headquartered in Oakland, California and is comprised of physician-owned, for-profit, partnerships, and professional corporations.

22. Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical Group, Inc. operate under the name "Kaiser Permanente," which is not a legal

entity but a registered trademark or trade name that Kaiser Foundation Health Plan, Inc. owns and Kaiser Foundation Health Plan, Inc., Kaiser Foundation Hospitals, and The Permanente Medical Group, Inc. use, acting in concert.

III. JURISDICTION AND VENUE

23. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 because this suit is brought under the laws of the United States, specifically the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq*. This Court also has subject matter jurisdiction under 28 U.S.C. § 1332(d)(2) because this a proposed class action in which there are at least 100 Class Members, the matter in controversy, exclusive of interest and costs, exceeds the sum or value of $5,000,000, and a member of the Class is a citizen of a different State than Defendant.

24. This Court also has supplemental jurisdiction over the state common law and statutory claims pursuant to 28 U.S.C. § 1367, as these claims are so related to the federal statutory claims over which this Court has original jurisdiction, that they form part of the same case or controversy.

25. This Court has general personal jurisdiction over Defendants because Defendants have sufficient minimum contacts with this District in that they operate and market their services throughout the region and in this District. Further, this Court has personal jurisdiction over Defendants because Defendants are headquartered in this District.

26. Venue properly lies in this District pursuant to 28 U.S.C. § 1391(a), (b), and (c) because: a substantial part of the events or omissions giving rise to Plaintiff's and the Classes' claims occurred in this District, Defendants conduct a substantial amount of business in this District, and Defendants are headquartered in this District.

IV. FACTUAL ALLEGATIONS

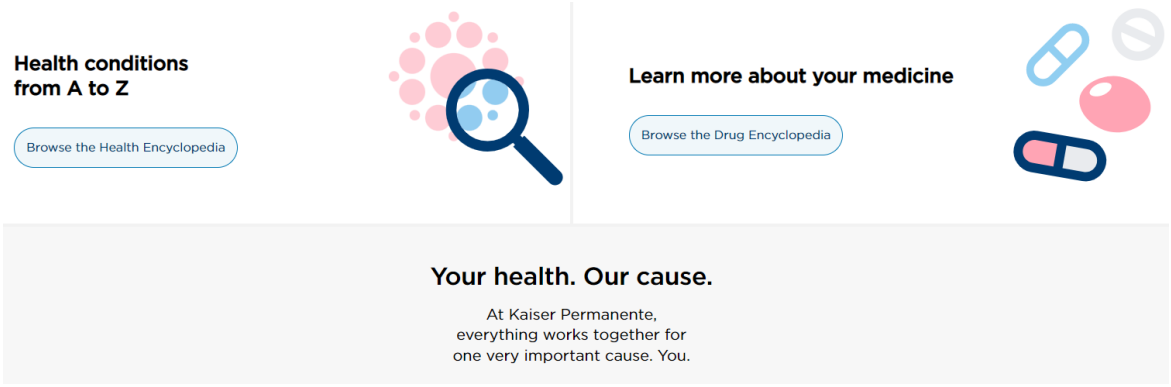
A. Kaiser Permanente Communicates with Kaiser Plan Members Through the Kaiser Permanente Website

27. Plaintiff and members of the Classes are Kaiser Plan Members.

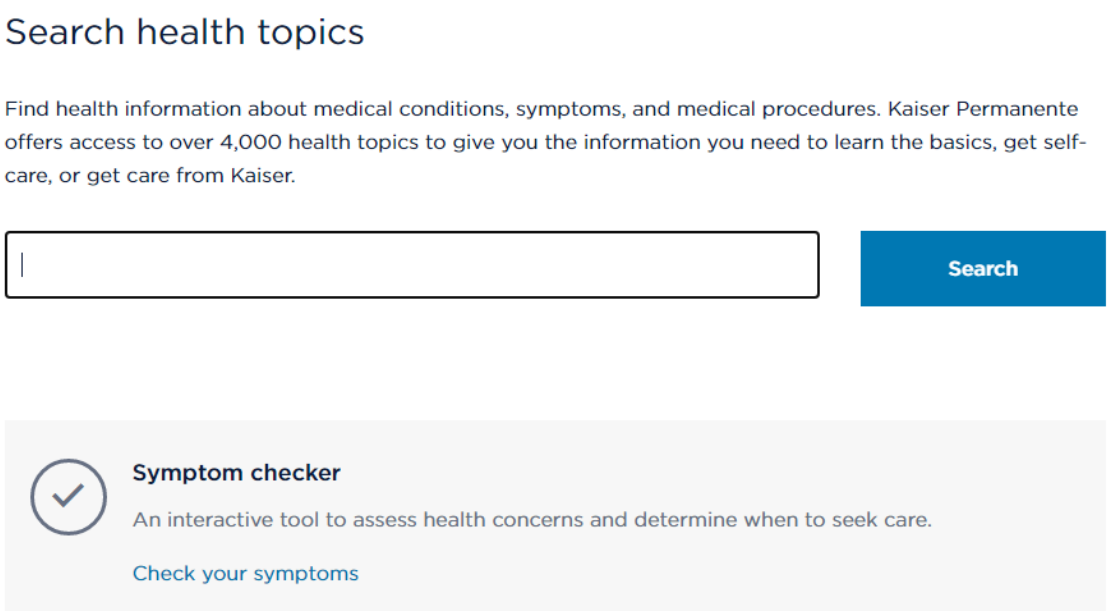
28. Kaiser Permanente operates a website ("Site"), with a homepage located at https://healthy.kaiserpermanente.org/front-door ("Homepage"), through which Kaiser Plan Members can perform various tasks that traditionally were only available by physically visiting their health

care providers' offices or speaking directly to their health care providers, such as scheduling appointments; checking medical results; reviewing medical histories; researching doctors, locations, and medical services; communicating with providers and paying medical bills.

29. The Site's Homepage provides Kaiser Plan Members and the public with information about the health care services that Kaiser Permanente offers, including links to find doctors and locations, get information about health conditions, and learn more about prescribed medicines.

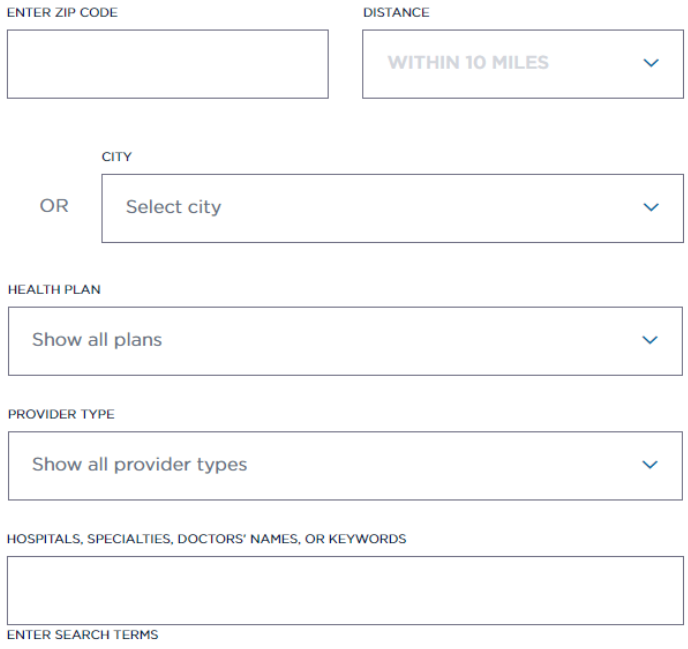


30. For example, on the Homepage, Kaiser Plan Members can click "Browse Health Encyclopedia" and access a page that allows them to find health information about certain medical conditions, symptoms and medical procedures, including over 4,000 health topics, by typing their health-related information into a search form. Kaiser Plan Members can also check their symptoms with an interactive "symptom checker" and "determine when to seek care."

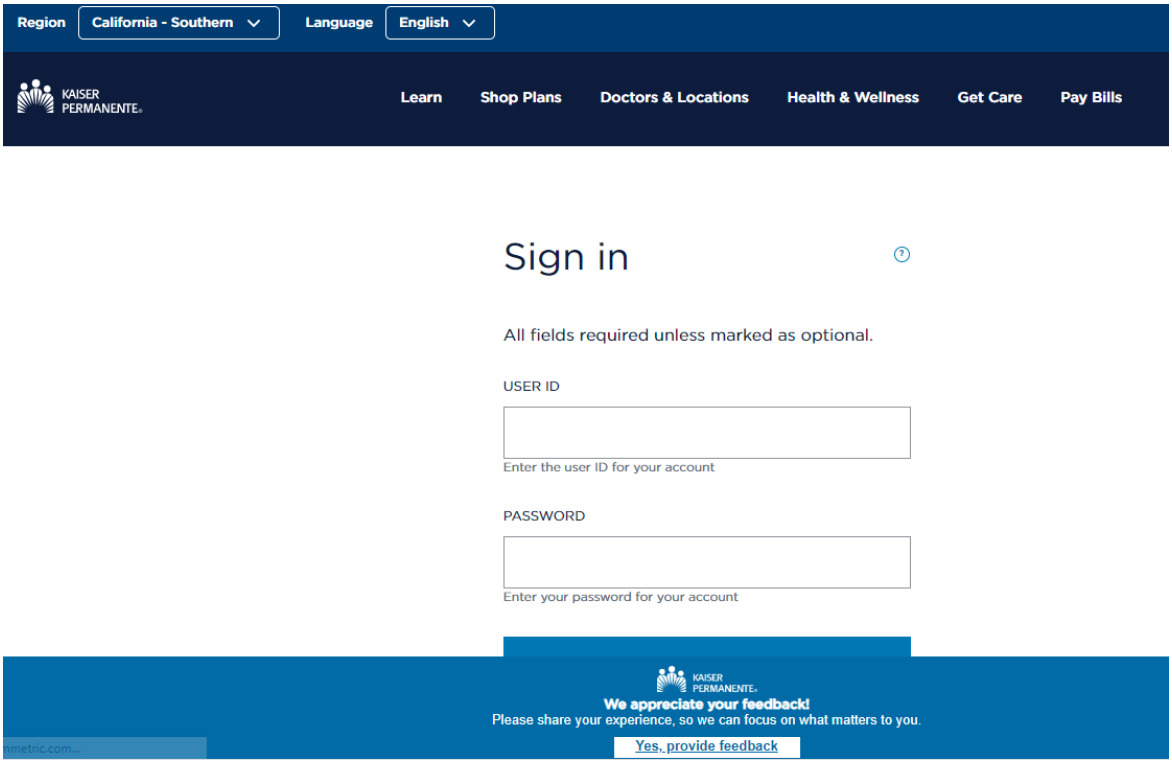


31. As the Site states, these topics and medical information provide Kaiser Plan Members with the information needed to "learn the basics, get self-care, or get care from Kaiser."

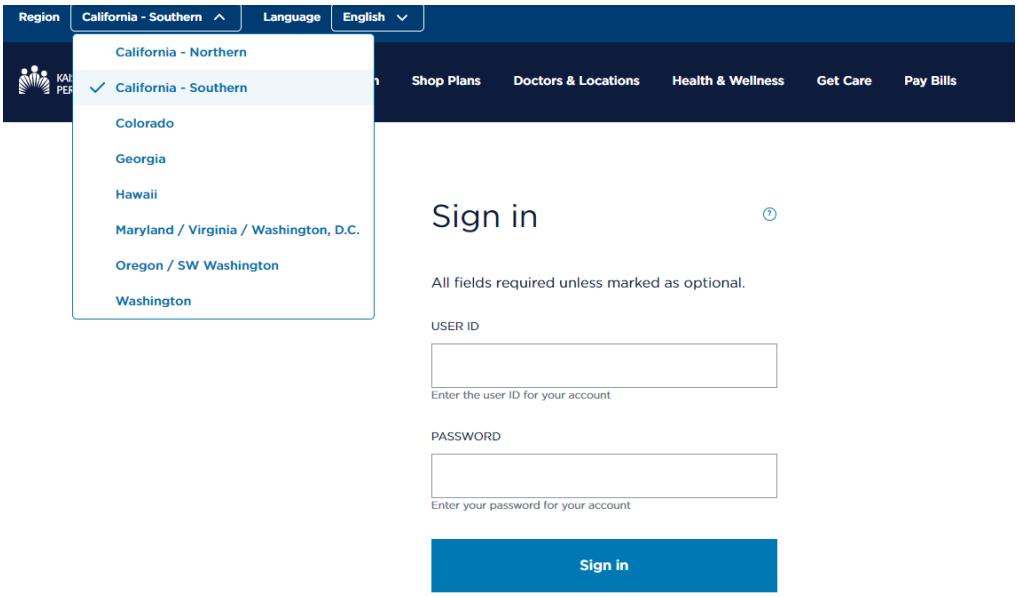
32. On the Homepage, Kaiser Plan Members can also click "Find a doctors or location" and access a form (https://healthy.kaiserpermanente.org/southern-california/doctors-locations#/search-form) where they can input their personal and health information to search for health care providers, including by location, specialty, or provider type or with particular keywords related to medical conditions or symptoms the Kaiser Plan Member is experiencing.



33. Kaiser Plan Members can also access their medical information, prescription information and test results, pay bills, schedule appointments, communicate with providers, and perform other actions related to their healthcare after clicking the "Sign In" Link for their region ("Portal Login Page") and accessing a purportedly secure patient Portal (the "Portal"). For example, if the Kaiser Plan Member, like Plaintiff, is located in Southern California, they can select "California – Southern" from a "Region" pulldown menu, click the "Sign In" link and be taken to the Portal Login page for Southern California located at https://healthy.kaiserpermanente.org/southern-california/consumer-sign-on#/signon:

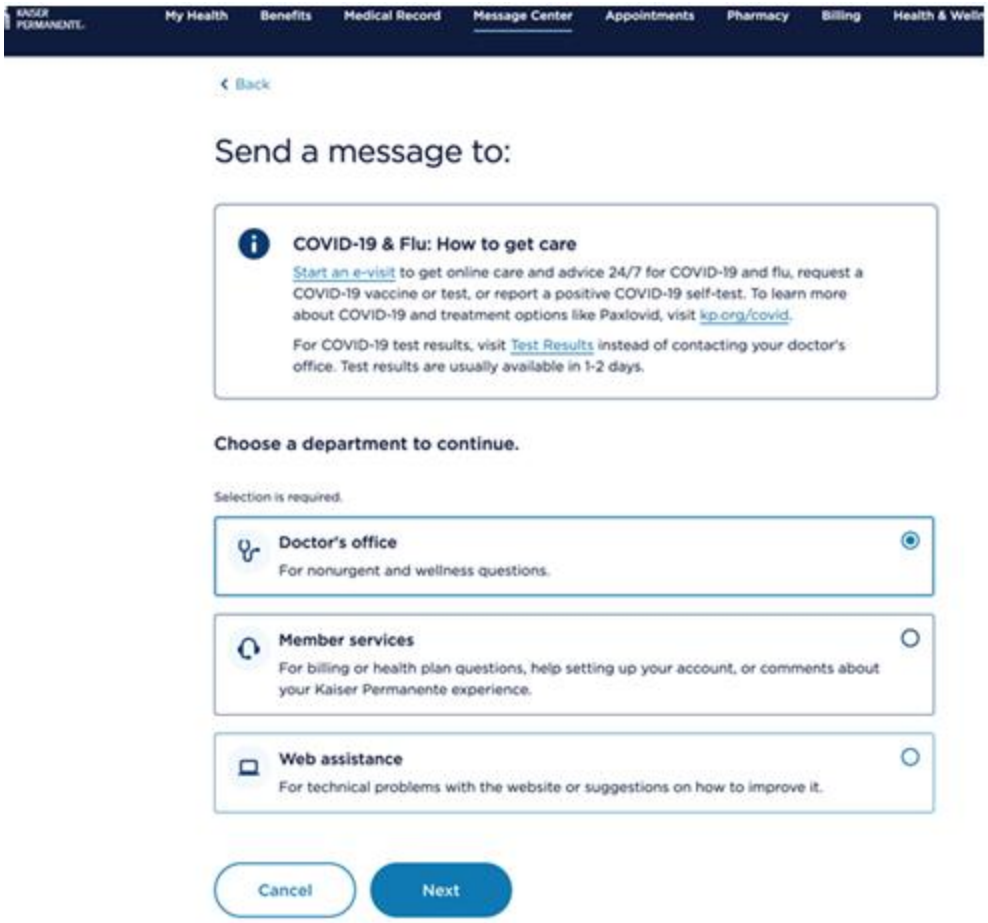


34. Kaiser Plan Members in Northern California, or other Regions such as Colorado, Georgia, Hawaii, Maryland/Virginia/Washington, D.C., Oregon/ S.W. Washington, and Washington can similarly select their region from a pulldown menu and access their Portal Login Page:

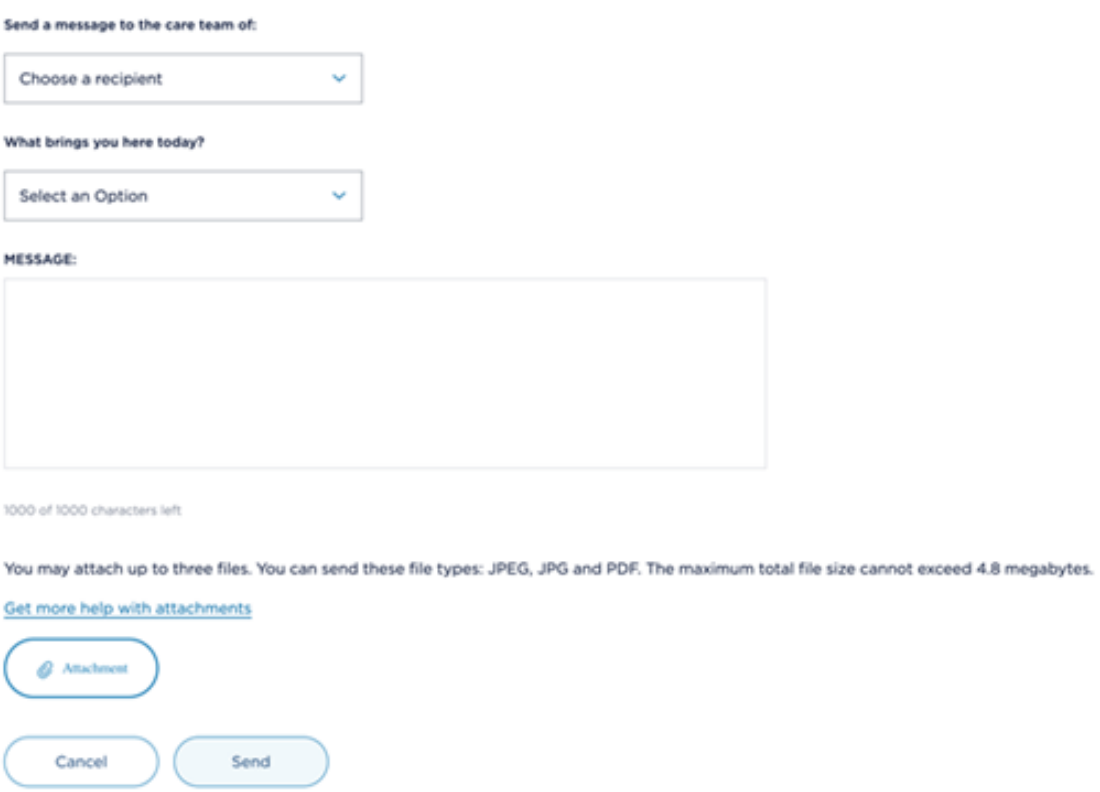


35. After signing into the Portal Login Page and entering the Portal, Kaiser Plan Members can access an array of services and view and provide personal and highly sensitive medical information, including viewing medical history, prescriptions, test results, scheduling appointments, performing online medical evaluations, researching symptoms, and communicating with providers, among other things.

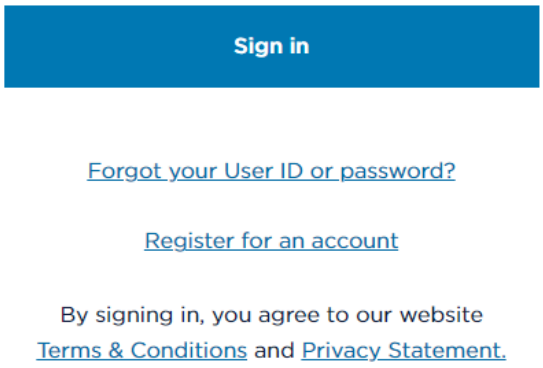
36. For example, the Portal contains a "Message Center" that allows Kaiser Plan Members to communicate directly with their health care providers:



37. After selecting a particular department, Kaiser Plan Members can identify specific recipients to whom they choose to communicate with and type out messages in a free form "Messages" box, with replies also sent and received within the Message Center.



38. The bottom of the Portal Login Page also provides: "By signing in, you agree to our website Terms & Conditions and Privacy Statement."



39. The Kaiser Permanente Terms & Conditions, available via hyperlink[4] and attached hereto as Exhibit 1, provides: "Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement."

[4] *See, e.g.*, *Terms & Conditions for our Website and Mobile Application*, Kaiser (Updated Jun. 2022), https://healthy.kaiserpermanente.org/southern-california/termsconditions.

40. The Kaiser Permanente Privacy Statement, also available via hyperlink[5] attached hereto as Exhibit 2, assures Kaiser Plan Members that Kaiser Permanente's data collection "is collected on an aggregate basis, which means that no personally identifiable information is associated with the data," which is untrue.

41. The Kaiser Permanente Privacy Statement also states that Kaiser Permanente and its service providers may place "cookies" or similar technologies on the computer hard drives of visitors to the Site, but falsely states that information obtained from cookies is only used to help Kaiser Permanente "tailor our Site to be more helpful and efficient for our visitors" when in fact the cookies are also being used for marketing purposes, unbeknownst to Kaiser Plan Members and without their permission or agreement.

42. The Kaiser Permanente Privacy Statement also falsely states that "[t]he cookie consists of a unique identifier that does not contain information about your health history," when in fact the information provided to the Third Party Wiretappers contains information about Kaiser Plan Members' health history.

43. The Kaiser Permanente Privacy Statement also states that Kaiser "may also occasionally use 'Web beacons' (also known as 'clear gifs,' 'Web bugs,' '1-pixel gifs,' etc.)" but falsely claims that Kaiser Permanente does "not collect any personal health information."

44. The Kaiser Permanente Privacy Statement also does not disclose to Kaiser Plan Members that Kaiser Permanente has aided, agreed with, employed, and/or conspired with, third parties that are recording the information that Kaiser Plan Members are sending, accessing, reviewing, or receiving through the Site.

45. Kaiser Permanente's website also contains a HIPAA Notice of Privacy Practices,[6] which purports to describe how and when Kaiser Permanente discloses information covered by HIPAA; however, nowhere in the HIPAA Notice of Privacy Practices does Kaiser Permanente

[5] *See, e.g., Website and mobile application Privacy Statement*, Kaiser, https://healthy.kaiserpermanente.org/southern-california/privacy (last visited Apr. 28, 2023).

[6] *See, e.g.*, *Notice of Privacy Practices*, Kaiser, https://healthy.kaiserpermanente.org/southern-california/privacy-practices (last visited Apr. 28, 2023).

disclose that it is providing HIPAA-protected and other confidential information to the Third Party Wiretappers.

46. Kaiser Permanente expressly and impliedly promises Kaiser Plan Members that it will maintain the privacy and confidentiality of the information shared, and the communications engaged in, on the Site and the Portal and that such information and communications will not be disclosed to or tracked by third parties.

47. Despite its express and implied assurances of privacy, Kaiser Permanente intentionally incorporated the Third Party Wiretappers' code and recording technology on the Kaiser Permanente website, and allowed the tracking and disclosure of Kaiser Plan Members' identifying information, personal and sensitive health information, and private, sensitive, and confidential communications with Kaiser Permanente and its providers to Third Party Wiretappers.

B. Multiple Third Party Wiretappers Intercept Kaiser Plan Members' Information Shared with, and Communications with, Kaiser Permanente and Its Providers

1. Kaiser Permanente Allows Quantum Metric to Intercept Kaiser Plan Members' Information and Communications

48. Unbeknownst to Kaiser Plan Members and against their reasonable expectations, Kaiser Permanents allows Quantum Metric to intercept Kaiser Plan Members' personal and sensitive identifying and medical information and confidential communications from the Site and Portal.

49. Kaiser Permanente has placed Quantum Metric's "Session Replay" code on its Homepage, Portal Login Page, and other pages on the Site—including within the Portal—which intercepts and records the contents of Kaiser Plan Members' information and confidential communications, and sends that information and those communications to Quantum Metric.

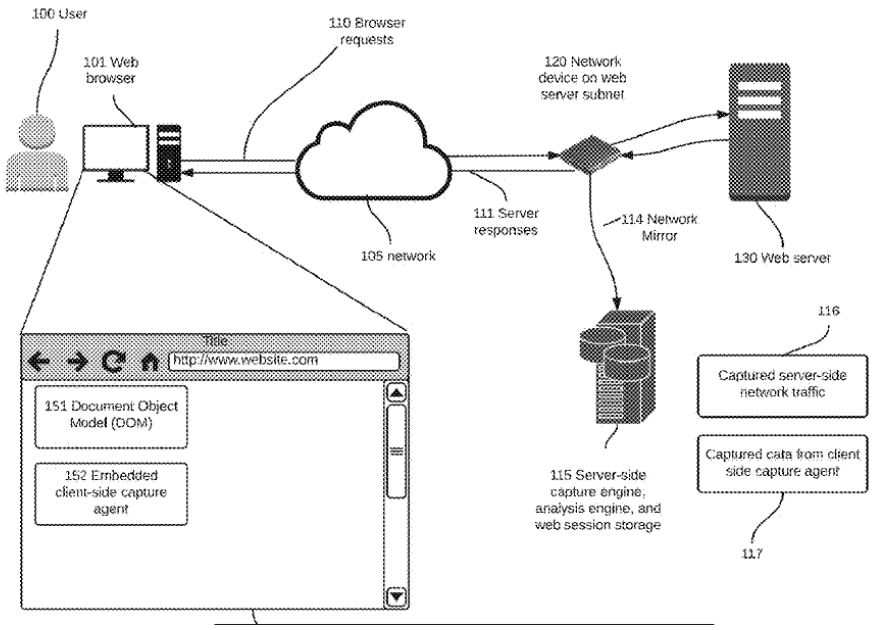
50. Quantum Metric collects and saves website communications, including those on the Site and Portal, through a service named "Session Replay." Session Replay captures internet communications between a website user and a website, including those on the Site and Portal, in real time while those communications are in transit.

51. As Quantum Metric explains: "At its core, **session replay** is technology that allows you to watch an end user's session as they experienced it, similar to how you watch a video. You can

pause, rewind, and fast-forward the session (just like a YouTube video) to watch how a user interacts with a website or mobile app."[7]

52. Session replay technologies work by using "embedded snippets of code . . . [that] watch and record a visitor's every move on a website, in real time."[8] This was done on the Site and the Portal when used by Kaiser Plan Members.

53. As illustrated in Quantum Metric's patent, after a user submits a communication to a web server, such as Kaiser Permanente's, Quantum Metric's embedded side capture agent code redirects the communications to Quantum Metric's server-side capture engine, analysis engine, and web session storage:



54. From the moment a Kaiser Plan Member loads Kaiser Permanente's website, Quantum Metric is intercepting all of the content viewed and communicated, as well as the Kaiser Plan Member's interactions with the website, similar to an individual peering over the user's shoulder and listening in on the patient's conversations with their medical provider.

[7] *What is Session Replay*, Quantum Metric, https://www.quantummetric.com/enterprise-guide-to-session-replay (last visited Apr. 28, 2023).
[8] Tomas Foltyn, What's the Deal with Session-Replay Scripts?, welivesecurity (Apr. 20, 2018, 1:40 pm), https://www.welivesecurity.com/2018/04/20/whats-deal-session-replay-scripts/.

55. As Kaiser Plan Members navigate the Kaiser Permanente Site, including accessing the Portal, the Site makes numerous "POST" calls to Quantum Metric, the size of which change based on site activity. A "POST" call is a HTTP method that sends user data to a server.

56. Thus, by installing the Quantum Metric Replay code on its website, Kaiser Permanente allowed Quantum Metric to intercept and record Kaiser Plan Members' identifying information, personal and sensitive medical information, including HIPAA-protected health information, and confidential communications with Quantum Metric's Session Replay code, in real time.

57. By way of example, on April 20, 2023, after Plaintiff logged into the Portal—which displayed his Name, Medical Record Number (Kaiser ID #), Region, and Coverage Status—but he performed no further activities, the amount of data intercepted and transferred to Quantum Metric (at kp-app.quantummetric.com) was about 16-32 bytes. Thereafter, when Plaintiff performed several activities within the Portal, the amount of the data transferred to Quantum Metric increased to over 125kB, indicating that Plaintiff's activity inside the Portal was being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

58. On April 20, 2023, after Plaintiff logged into the Portal and then accessed the Doctor Search Page and performed no further activities, the amount of data intercepted and transferred to Quantum Metric was 15 bytes. Thereafter, when Plaintiff entered personal medical search information into the Doctor Search page, the amount of data transferred to Quantum Metric increased to over 60kB, indicating that Plaintiff's medical search information was being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

59. On April 20, 2023, when Plaintiff accessed the E-visit page within the Portal and answered various questions as part of an E-visit mental health assessment session, the amount of data transferred to Quantum Metric was over 42kB, indicating that Plaintiff's personal information and private and confidential answers to questions during the E-visit mental health assessment, were being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

60. On April 20, 2023, when Plaintiff accessed the Site's health encyclopedia after logging into the Portal and searched on mental health topics, the amount of data transferred to Quantum Metric was over 670kB, indicating Plaintiff's personal information and private and confidential communications about mental health topics was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

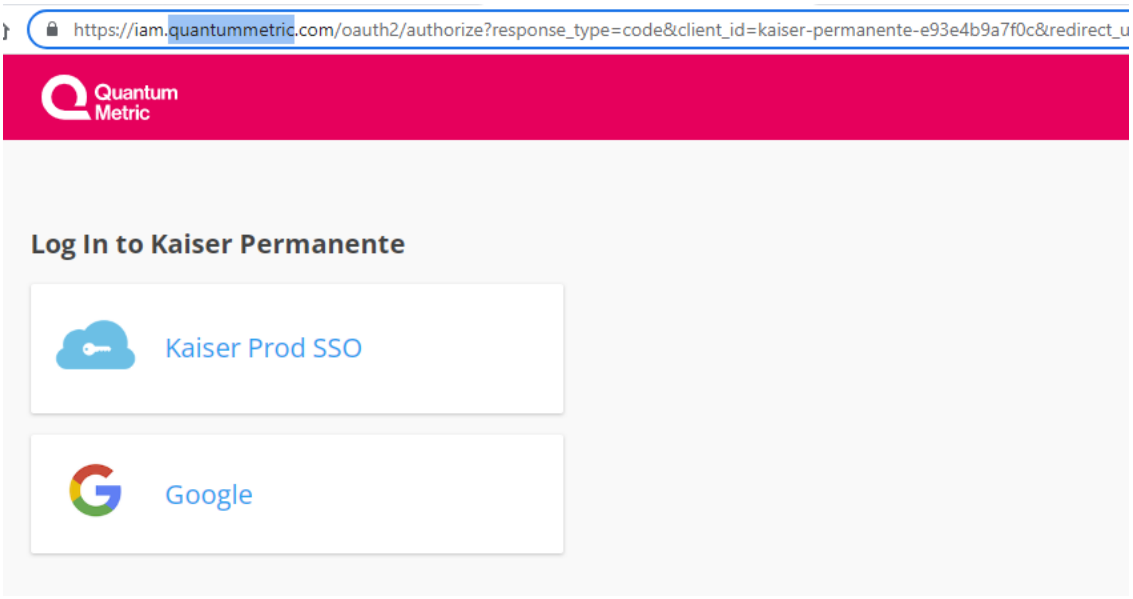
61. On April 21, 2023, when Plaintiff again logged into the Portal and accessed recent medical test results, the amount of data transferred to Quantum Metric was over 225kB, indicating that information about Plaintiff's personal and sensitive identifying and medical information, and private and confidential medical test results, was also being intercepted by Quantum Metric and redirected to kp-app.quantummetric.com.

62. On information and belief, the same type of information tracked, disclosed, and sent to Quantum Metric for Plaintiff has been tracked, disclosed, and sent to Quantum Metric for other members of the Classes.

63. Additionally, when Kaiser Plan Members navigate other portions of the Site, Quantum Metric intercepts and receives that content as well. For example, if a patient searches for doctors who specialize in Addiction Medicine, Quantum Metric will receive the search results displaying this sensitive information, as well as data regarding all of the information the Kaiser Plan Members provided and received regarding that topic.

64. For example, on April 20, 2023, after Plaintiff logged-off of the Portal, Plaintiff again conducted a doctor search, viewed the Homepage (Southern California region), and accessed the health encyclopedia on the Site. In all cases, Plaintiff's actions and data were intercepted by Quantum Metric and transferred to kp-app.quantummetric.com.

65. The recordings of Plaintiff and other Class Members' information and confidential communications on the Site are saved on Quantum Metric's systems and are available for viewing on Quantum Metric's website, an example of which is below:



66. Kaiser Permanente voluntarily embedded Quantum Metric's software code on the Site, knowing that Quantum Metric's software would intercept, record, and redirect Kaiser Plan Members' Site and Portal activity, including personal health information and/or HIPAA-protected information and communications with Kaiser Permanente and its providers.

67. Unlike certain other third parties, Quantum Metric does not only receive website analytics data that provides aggregate statistics; rather, the Quantum Metric recording technology utilized by Kaiser Permanente is intended to record and playback individual browsing sessions, as well as the private and confidential information and communications shared in those sessions. The monitoring that Quantum Metric's technology provides extends beyond the computer "cookies" with which ordinary consumers may be familiar.

68. Moreover, the collection and storage of Kaiser Plan Members' communications with their health care providers may cause sensitive health information and other personal information displayed on a page to leak to additional third parties. This may expose Kaiser Plan Members who use the Site and/or Portal to identity theft, online scams, and other unwanted behavior.

69. In a 2017 study by Princeton University's Center for Information Technology Policy concerning session recording technologies, the researchers noted "[c]ollection of page content by third-party replay scripts may cause sensitive information such as medical conditions, credit card details and other personal information displayed on a page to leak to the third-party as part of the

recording. This may expose users [like Plaintiff and members of the Classes] to identity theft, online scams, and other unwanted behavior."[9]

70. The study goes on to state that "the extent of data collected by these services far exceeds user expectations; text typed into forms is collected before the user submits the form, and precise mouse movements are saved, all without any visual indication to the user. This data can't reasonably be expected to be kept anonymous."[10]

71. As currently deployed, Quantum Metric's recording function, as employed by Kaiser Permanente, functions as a wiretap, and Quantum Metric acts as a third-party wiretapper.

2. Kaiser Permanente Allows Adobe to Intercept Kaiser Plan Members' Information and Communications

72. Unbeknownst to Kaiser Plan Members and against their reasonable expectations, Kaiser Permanente allows Adobe to intercept Kaiser Plan Members' information and communications from the Site and Portal.

73. Kaiser Permanente allows Adobe to intercept Kaiser Plan Members' personal and sensitive identifying and medical information and private and confidential communications through code connected with the Adobe Experience Cloud a/k/a Adobe Marketing Cloud service embedded on the Site, including within the Portal.

74. The Adobe Experience Cloud service is a suite of products offered by Adobe, which allow businesses to personalize and improve their marketing on websites, apps, and social media pages by collecting and analyzing information about website visitors.

75. The Adobe Experience Cloud includes a number of services including: Measurement solutions, which allows companies to measure and understand visitors who use their websites, apps, and social media pages, as well as how they interact with online marketing campaigns; Personalization solutions, which allows companies to test new content and make their websites, apps, social media pages, and emails more relevant to particular visitors; Content management solutions,

[9] Steven Englehardt, *No boundaries: Exfiltration of personal data by session-replay scripts*, Freedom to Tinker (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

[10] *Id.*

which allows companies to store, update, and deliver images and other content on their websites, within their apps, and in online marketing materials; and Advertising solutions, which allows companies to improve their online advertising on websites, apps, search engines, and social media, including helping companies send emails, text messages, and other online and offline marketing campaigns.[11]

76. The Adobe Experience Cloud collects an array of information about website visitors, including:

- Where you go and what you do on that company's websites, apps, or social media pages
- Your web browsing activity, including the URLs of the company's web pages you visit
- The URL of the page that displayed the link that you clicked on, which brought you to that company's website
- The web search you performed that led you to that company's website
- Information about your web browser and device, such as device type, browser type, advertising identifier, operating system, connection speed, and display settings
- Your IP address (or partial IP address, depending on how the company has configured the solution), which may be used to approximate your general location
- Location information from your mobile device or web browser
- Social media profile information
- Information you may provide on that company's website, app, or when interacting with that company's social media pages, such as information you provide on registration forms
- Ad campaign success rates, such as whether you clicked on a company's ad and whether viewing or clicking on the ad led to your purchase of that company's product or service
- Items you've purchased or placed in your shopping cart on that company's website or app[12]

77. As part of the Adobe Advertising Cloud solution, Adobe makes available certain health-related segments supplied by third-party data providers to the companies using the Adobe Advertising Cloud, allowing companies to use these segments to target ads when they are using the Adobe Experience Cloud. These data segments generally fall into the following categories: (1) occupation in a health related field, (2) health related topics and conditions, (3) interest in health

[11] *Adobe Experience Cloud privacy*, Adobe (Updated Dec. 5, 2022), https://www.adobe.com/privacy/experience-cloud.html.

[12] *Id.*

insurance, (4) diet, fitness, weight-loss, and healthy lifestyles, (5) consumer goods and services for personal healthcare, vision care, grooming, and beauty, (6) over the counter medicines, remedies, and dietary supplements, and (7) health related charities.

78. The Adobe Experience Cloud collects this information through an array of tracking technologies, including cookies and/or web beacons (also known as tags or pixels), such as the third party cookies omtrdc.net, demdex.net, and the Adobe Experience Platform Launch, which delivers a library containing specified tags for other Adobe Experience Cloud solutions.[13]

79. As Kaiser Plan Members navigate the Kaiser Permanente Site, the Site makes numerous "POST" calls which send information about Kaiser Plan Members' confidential communications with Kaiser Permanente to Adobe.

80. Adobe has established subdomains on its own server, such as the subdomain kaiser.tt.omtrdc.net on Adobe's omtrdc.net server, where Adobe receives and stores the communications intercepted from Kaiser Permanente.[14]

81. For example, on April 20, 2023, after Plaintiff logged into the Portal, the following data was intercepted by Adobe and sent to Adobe's server at the kaiser.tt.omtrdc.net subdomain, which as detailed below shows that Adobe received a host of personally identifiable health information, including: user data (color coded in blue), the URL of the Website the user is currently browsing (color coded in green), unique IDs (color coded in yellow), customer IDs and status values (color coded in grey),[15] and segmentation values that enable the Website to show personalized content (no color).

{"requestId":"107119803ed046f6b5b7a4720cb69916","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Chromium\";v=\"112\", \"Google Chrome\";v=\"112\", \"Not:A-Brand\";v=\"99\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":3008,"height":1692,"orientation":"landscape","colorDepth":24,"pixelRatio":2},"window":{"width":1992,"height":1002},"browser":{"host":"healthy.kaiserpermanente.org","we

[13] This includes cookies identified as "everest_g_v2" and "demdex.net", which aid in tracking users. According to Adobe's marketing materials, the everest_g_v2 cookie is "created after a user initially clicks a client's ad, and used to map the current and subsequent clicks with other events on the client's website."

[14] *Adobe Experience Cloud privacy*, *supra* note 10.

[15] Specific identifier number have been redacted.

bGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/secure/inner-door","referringUrl":""}},"id":{"tntId":"Redacted","thirdPartyId":"15173479","marketingCloudVisitorId":"Redacted","customerIds":[{"id":"Redacted","integrationCode":"kpaamidepp","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"6G1ynYcLPuiQxYZrsz_pkqfLG9yMXBpb2zX5dvJdYQJzPXImdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"Redacted"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:inner-door","Seg114v cookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":5579818,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg516e":false,"Seg126v":false,"modval":8,"Seg21":299028,"Seg22":"https://healthy.kaiserpermanente.org/southern-california/secure/inner-door","Seg24":"urn:kp:prodvam","Seg25":"","entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"54","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":5579818,"Seg12":"ACTIVE","Seg101v":51,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"Redacted","Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:inner-door","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":5579818,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg516e":false,"Seg126v":false,"modval":8,"Seg21":299028,"Seg22":"https://healthy.kaiserpermanente.org/southern-california/secure/inner-door","Seg24":"urn:kp:prodvam","Seg25":"","entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"54","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":5579818,"Seg12":"ACTIVE","Seg101v":51,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"Redacted","Seg103v":false}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1682016685321,"execution":19.7},{"execution":234.1,"parsing":0.1,"request":{"tls":1,"timeToFirstByte":218.9,"download":0.6,"responseSize":2641},"telemetryServerToken":"y6ggVo6+nhjp+nYzHbCsfoQ5YLKNHYN2xE+jRXv79rQ=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"047a8d8c010a44ca959428b10b74b05d","timestamp":1682016685299}]}}

82. The first block color coded in blue is sent as part of the HTTP request header and is used to create a digital fingerprint for the specific user by collecting information about the specific user's browser and device information, including details about the user's browser type, computing device, operating system, screen height and width, and details about the user's graphics card.

Together these details create a device fingerprint[16] which allows Adobe to compile and track long-term records of the individual's browsing history (and thus deliver targeted advertising or targeted exploits) even when visitors are attempting to avoid tracking—raising a major concern for internet privacy advocates.

83. The second block (green) indicates the URL for the Webpage currently visited by the user. Here, Adobe is receiving information that Plaintiff has logged-into the Portal, signifying that Plaintiff is a Kaiser Plan Member and Kaiser Permanente Patient—information which Kaiser Permanente is prohibited from disclosing under HIPAA and other state and federal laws.

84. The third block (yellow) includes three identifiers set by Adobe: (1) marketingCloudVisitorID, (2) tntID, and (3) thirdPartyID. These identifiers work in tandem with the demdex.net server and the AMCV cookie to help specifically identify users.

85. When a user first visits a site with the Adobe Experience Cloud installed, like when Kaiser Plan Members visit the Site and/or Portal, Adobe checks to see if the AMCV cookie is set. This cookie stores the marketingCloudVisitorID (also known as Experience Cloud ID). According to Adobe, the marketingCloudVisitorID "is a universal and persistent ID that identifies your visitors across all solutions in the Experience Cloud."[17] In the POST called referenced above the marketingCloudVisitorID is assigned a specific numeric value ([redacted]). This in turn allows for tracking of Kaiser Plan Members across Kaiser Permanente sites and across devices.

86. If the AMCV cookie is not set, the Adobe code places a call to the demdex.net server, which generates a marketingCloudVisitorID and sets the AMCV cookie with that value. It also sets a demdex ID cookie which is persistent.[18] Since the marketingCloudVisitorID is stored in the AMCV cookie, it will remain the same for anyone using the browser for that specific site. When a user visits another site with Adobe Experience Cloud installed, a new marketingCloudVisitorID will be

[16] Fingerprinting, web.dev, https://web.dev/learn/privacy/fingerprinting/ (last visited Apr. 28, 2023).
[17] *Adobe Target Delivery API (1.0.0) Terms of Service*, Adobe, https://developers.adobetarget.com/api/delivery-api/#section/Identifying-Visitors (last visited Apr. 28, 2023).
[18] *How the Experience Cloud Identity Service requests and sets IDs*, Adobe (Updated Nov. 10, 2022), https://experienceleague.adobe.com/docs/id-service/using/intro/id-request.html?lang=en.

generated, but the demdex ID will remain the same. According to Adobe, "the demdex ID remains the same . . . because it's contained in a third-party cookie and persists across different domains."[19] This in turn allows Adobe to track specific devices across sites.

87. According to Adobe the tntID, "can be seen as a device ID."[20] As detailed above, device IDs use the unique setup of a user's computer and browser to establish a device fingerprint. This fingerprint can track users across various Websites to build a profile based on their Web browsing habits. In the POST call referenced above the tntID is assigned a specific numberic value ([redacted]). The tntID is stored in the persistent mbox cookie. Adobe uses the tntID as the main identifier for its Adobe Target solution.[21] The Adobe Target system is used to personalize a user's experience on a website, like Kaiser Plan Members on the Site and Portal. By default, Adobe Target captures the following data, which in turn allows the website to serve personalized and targeted information to specific users:

Data category	Description
Environment parameters	Information about a user's environment, including operating system, browser, and time of day/day of week.
Geography	Information about a user's geography, obtained via IP lookup.
Mobile device	Information about a user's mobile device.
Target reporting segments	Reporting segments configured in Target reporting.
Session behavior	Information about user behavior, such as number of pages viewed.[22]

88. According to Adobe, the thirdPartyID "is a persistent ID that your business utilizes to identify an end-user regardless of whether they are interacting with your business from web, mobile, or IoT channels. In other words, the thirdPartyId will reference user profile data that can be utilized

[19] *Id.*
[20] *Adobe Target Delivery API (1.0.0) Terms of Service*, *supra* note 15.
[21] *Id.*
[22] Adapted from: *Data used by Target machine-learning algorithms*, Adobe (Updated Apr. 23, 2023), https://experienceleague.adobe.com/docs/target/using/activities/automated-personalization/ap-data.html

across channels."[23] In the POST call referenced above the thirdPartyId is assigned a specific numeric value (Redacted). This ID can be used to identify return users once they have logged into the Portal. This in turn allows Adobe's customers to associate the thirdPartyID with a specific individual, the third party here being Kaiser Permanente's patients.

89. The fourth block (grey) includes customerIds that can be, "added and associated with an Experience Cloud Visitor ID."[24] In the case of the POST call above, the additional data includes the fact the user is authenticated (logged in), again signifying that Plaintiff is a Kaiser Plan Member and Kaiser Permanente patient—information which Kaiser Permanente is prohibited from disclosing under HIPAA and other state and federal laws and its express and implied contracts with Kaiser Plan Members.

90. Similar POST calls to kaiser.tt.omtrdc.net were found on all examined pages, including main page (Southern California), doctor search, mental health encyclopedia, e-visit, and retrieving test results.

91. For example, after Plaintiff logged into the Portal and accessed test results on April 21, 2023, Adobe intercepted and received information about the medical procedure that Plaintiff was inquiring about, specifically a shoulder x-ray (see yellow highlight), which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

{"requestId":"d8acce0cfb0c4788ae7d98c9b6773713","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Chromium\";v=\"112\", \"Google Chrome\";v=\"112\", \"Not:A-Brand\";v=\"99\""},"timeOffsetInMinutes":-420,"channel":"web","screen":{"width":3008,"height":1692,"orientation":"landscape","colorDepth":24,"pixelRatio":2},"window":{"width":1663,"height":1513},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/secure/search-medical-record?uri=search%3ahealth-encyclopedia&type=CPT&query=73030&label=X%2DRAY+SHOULDER","referringUrl":"https://healthy.kaiserpermanente.org/va/inside.asp?mode=labdetail&eorderid=Redacted"}},"id":{"tntId":"af8d349f37b54d30abbfcb86f2f2830e.35_0","thirdPartyId":"15173479","marketingCloudVisitorId":"78520597070824876881305257068400971788","customerIds":[{"id":"Redacted","integrationCode":"kpaamidepp","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":

[23] *Adobe Target Delivery API (1.0.0) Terms of Service*, *supra* note 15.
[24] *Id.*

"kpaamidudr","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"kpaamid_One-off-datasets","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"pzn_crm","authenticatedState":"authenticated","type":"DS"},{"id":"Redacted","integrationCode":"mbox3rdPartyId","authenticatedState":"authenticated","type":"DS"}]},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"Redacted"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":5579818,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg516e":false,"Seg126v":false,"modval":8,"Seg21":299028,"Seg22":"","Seg24":"urn:kp:prodvam","Seg25":"","entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"54","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":5579818,"Seg12":"ACTIVE","Seg101v":51,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"Redacted","Seg103v":false}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"sca","Seg55v":"Logged In","Seg181v":"","Seg81v":"kporg:secure:search-medical-record","Seg114vcookie":"mbr","reEnable":"","throttle-area":"","Seg180v":false,"Seg4":true,"Seg517e":false,"Seg5":false,"Seg6":false,"Seg7":false,"Seg8":false,"Seg440e":false,"Seg9":false,"Seg11":false,"Seg20v":5579818,"Seg114v":"SUBSCRIBER","Seg13":false,"Seg14":false,"Seg16":false,"Seg19":false,"Seg516e":false,"Seg126v":false,"modval":8,"Seg21":299028,"Seg22":"","Seg24":"urn:kp:prodvam","Seg25":"","entitlement-446":true,"pLoaded":1,"id":""},"profileParameters":{"region":"","Seg2":"54","Seg56v":"MBR","Seg10":"NOT ENROLLED","Seg20v":5579818,"Seg12":"ACTIVE","Seg101v":51,"Seg15":"true","Seg106v":"KFHP_HMO","Seg6":"false","pzn_id":"Redacted","Seg103v":false}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1682104634267,"execution":13.8},{"execution":56,"parsing":0.1,"request":{"tls":0.9,"timeToFirstByte":49.7,"download":0.7,"responseSize":1565},"telemetryServerToken":"GRgdNPKF2baxcRHAQqAHqyTPswyQefSCMFGH9GY2aUI=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"a241e476537c46ee889a2bd5ea8970a2","timestamp":1682104634251}]}}

92. On April 20, 2023, when Plaintiff was logged out of the Portal and conducted a search on the Site's encyclopedia page for mental health, Adobe intercepted and received the following data (highlighted in yellow), which includes the various personal IDs detailed above (such as Plaintiff's tntID and marketingCloudVisitorID) and discloses the fact that Plaintiff had requested information from Kaiser Permanente regarding "mental health," which was transmitted to Adobe and stored on Adobe's kaiser.tt.omtrdc.net server:

{"requestId":"ce17897a88f94df8911b81e1dbf35ecd","context":{"userAgent":"Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.0.0 Safari/537.36","clientHints":{"mobile":false,"platform":"macOS","browserUAWithMajorVersion":"\"Chromium\";v=\"112\", \"Google Chrome\";v=\"112\", \"Not:A-Brand\";v=\"99\""},"timeOffsetInMinutes":-

420,"channel":"web","screen":{"width":3008,"height":1692,"orientation":"landscape","colorDepth":24,"pixelRatio":2},"window":{"width":1992,"height":1357},"browser":{"host":"healthy.kaiserpermanente.org","webGLRenderer":"ANGLE (Apple, Apple M1 Pro, OpenGL 4.1)"},"address":{"url":"https://healthy.kaiserpermanente.org/southern-california/pages/search?query=mental+health&category=global&global-region=sca&language=english&region=sca","referringUrl":"https://healthy.kaiserpermanente.org/southern-california/health-wellness/health-encyclopedia"}},"id":{"tntId":"Redacted","marketingCloudVisitorId":"Redacted"},"experienceCloud":{"audienceManager":{"locationHint":9,"blob":"RKhpRz8krg2tLO6pguXWp5olkAcUniQYPHaMWWgdJ3xzPWQmdj0y"},"analytics":{"logging":"server_side","supplementalDataId":"Redacted"}},"execute":{"pageLoad":{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:pages:search","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"54"}}},"prefetch":{"views":[{"parameters":{"Seg18v":"sca","Seg17v":"","Seg55v":"Logged Out","Seg181v":"","Seg81v":"kporg:pages:search","Seg114vcookie":"","reEnable":"","throttle-area":""},"profileParameters":{"region":"","Seg2":"54"}}]},"telemetry":{"entries":[{"requestId":3198432,"timestamp":1682019482663,"execution":20.9},{"execution":203,"parsing":0.1,"request":{"tls":1.2,"timeToFirstByte":196.8,"download":0.3,"responseSize":1842},"telemetryServerToken":"sWzAuPN0jRUiKvgomAHTp5Xnsnn8TJkKAI00wNaSyq4=","mode":"edge","features":{"executePageLoad":true,"prefetchViewCount":1,"decisioningMethod":"server-side"},"requestId":"90b30902cc1a457bbbf75df338f3a4d6","timestamp":1682019482638}]}}

93. On information and belief, the same type of information tracked, disclosed, and sent to Adobe for Plaintiff has been tracked, disclosed, and sent to Adobe for other members of the Classes.

3. Kaiser Permanente Allows Twitter, Bing, and Google to Intercept Patients' Communications

94. Kaiser Permanente, on its Home Page, Portal Login Page, and other pages on the Site—including within the Portal—also uses code that sends confidential and protected health information to Twitter, Bing, and Google.

95. Google and Bing are the most widely used search engines, and Twitter is one of the largest social media sites in the world.

96. Generally, Google, Bing, and Twitter do not charge to use their services because they are able to generate billions of dollars in revenue each year by selling targeted advertising.

97. For example, if a user tweets about a current event in the news or about their job, Twitter and advertisers can understand a user's political leanings or job type. This information is

valuable to Twitter because it helps advertisers understand who Twitter users are so that Twitter can sell advertisements targeting that particular user's Twitter timelines.[25]

98. Twitter also tracks browsing activity outside of Twitter, for both Twitter users and people who have never created an account on the Twitter platform, including browser type, the device and operating system, the mobile carrier, IP address, and browsing activity.[26] Twitter can also learn information about websites visited before landing on the referring website and what websites were visited after leaving the site.[27]

99. Google and Bing sell ads based on a user's search. So, a search for a medical condition such as cancer, would show ads for cancer treatment centers.

100. Google and Bing are also widely used ad platforms that provide ad remarketing. Remarketing shows ads based on sites a user has previously visited. For example, a user who visits a website with Google or Bing code, and searches on pregnancy related topics, might then see ads for a Google or Bing advertiser's pregnancy related services on other websites.

101. A main goal for Google, Bing, and Twitter is to develop a profile of users to better target them with ads. Therefore, all these sites offer free analytics tools. These tools are useful to advertisers as they can show how effective certain ads are. Web analytics tools also provide general information about who is visiting the website and what those users are doing on the site.

102. The Kaiser Permanente Site, including inside the Portal, uses Bing Ads and Google and Twitter analytics. The Kaiser Permanente Website, including inside the Portal, also tracks views via integration with Doubleclick, which is owned by Google.

103. Bing, Google, and Twitter send data to their respective servers via HTTP GET request parameters.

104. The HTTP GET method requests data from a server. This request can include additional parameters that are sent as part of the request URL. For example, take the request "www.example.com ?utm_source=google." In this case, everything after the "?" is used to track

[25] Mehak Siddiqui, *What Does Twitter Know About Me?*, vpnoverview (Sept. 9, 2022), https://vpnoverview.com/privacy/social-media/what-does-twitter-know-about-me/.
[26] *Id.*
[27] *Id.*

where the site visitor came from, in this case showing that the visitor came from Google before accessing the www.example.com.

a) Portal Login

105. On April 20, 2023, when Plaintiff logged into the Portal, Bing sent the following GET request to bat.bing.com (color coded here and described in more detail below):

> https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=1ae9f073-60a4-44f7-bce9-43d2cf4488fe&sid=294d9520dfab11edaa7d1755dd644c7f&vid=294dbe90dfab11ed9ef7ad76fb5ac623&vids=0&msclkid=N&pi=9[Redacted]&lg=en-US&sw=3008&sh=1692&sc=24&tl=My%20Health%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&r=&lt=529&evt=pageLoad&sv=1&rn=447477

106. The Bing GET request includes temporary and session IDs (mid, sid, vid)—highlighted in yellow above, an indication that the page loaded (green highlight), the URL of the page (blue highlight), information about the browser and device (grey highlight) and a hash (pi) (pink highlight)—of the device data. As discussed above, hashes such as this are used to establish a device fingerprint to track devices across multiple websites. The data sent to Bing indicates the user successfully logged into the Portal.

107. According to Bing documentation, "the cookie in the relevant domain and IP address are always passed with every http request and not just via UET."[28] UET is Universal Event Tagging and it's the method used by Bing to report advertiser activity on a Website. UET was installed on all pages viewed on the Kaiser Website, including within the Portal.

108. When Plaintiff logged into the Portal, Google also sent multiple GET requests to both googleads.g.doubleclick.net and google.com. These requests are essentially similar in nature. For example, the data sent via GET to Google servers at googleads.g.doubleclick.net is below:

> https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1682016746120&cv=11&fst=1682016746120&bg=ffffff&guid=ON&async=1&gtm=45be34c0&u_w=3008&u_h=1692&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=My%20Health%20%7C%20Kaiser%20Permanente&auid=1394501439.1682016175&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

[28] https://help.ads.microsoft.com/apex/index/3/en/53056/

109. The above GET request includes the URL of the current site (blue highlight), the event type (highlighted in green)—in this case a conversion, as well as data about the browser and device that allows Google to produce a device fingerprint (highlighted in grey). The data sent to Google indicates the user successfully logged into the Portal.

110. When Plaintiff logged into the Portal, Google used the POST method to transmit the following data to Google servers at www.google-analytics.com:

> https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je34c0&_p=941729214&cid=1604752619.1682016174&ul=en-us&sr=3008x1692&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&_s=3&sid=1682016174&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fconsumer-sign-on&dt=My%20Health%20%7C%20Kaiser%20Permanente&en=user_engagement&_et=8100

111. The POST above includes temporary and session IDs (tid, cid, sid)—highlighted in yellow, an indication that the page loaded (green highlight), the URL of the current page (blue highlight), and information about the browser and device (grey highlight). As discussed above, device data allows Google to establish a device fingerprint to track devices across multiple websites. The data sent to Google indicates the user successfully logged into the Portal.

112. When Plaintiff accessed the Portal, Twitter sent two GET requests—one to analytics.twitter.com and one to t.co. Except for the base domain, both GET requests were the same as follows:

> https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=b7251997-28cf-4dcc-9926-53d9a01ba6c1&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=bb45caa1-c7d9-4d71-893c-b875d9fef676&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Finner-door&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

113. As reflected above, highlighted in blue, the Twitter GET requests were used to indicate a page view of the Portal—indicating the user successfully logged in.

b) Inside the Portal—Accessing Test Results

114. On April 21, 2023, when Plaintiff accessed test results from within the Portal, Bing, Google, and Twitter all transmitted the fact that Plaintiff has a shoulder X-ray in their GET requests back to their respective servers.

115. For example, Bing's GET request from the test results page was:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=6fff0767-39ee-4add-b2c8-400f112dd65b&sid=294d9520dfab11edaa7d1755dd644c7f&vid=294dbe90dfab11ed9ef7ad76fb5ac623&vids=0&msclkid=N&pi=9[Redacted]&lg=en-US&sw=3008&sh=1692&sc=24&tl=Search%20medical%20records&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&r=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fva%2Finside.asp%3Fmode%3Dlabdetail%26eorderid%3DWP-24V-2B3NQ2bC6-2BleBI3Fg9nA2psYu22GNxSPpkW8KgU5hKk-3D-24RP2b0miWDEm9WTRBUztJc9Ww7w1Jn-2FJdxlN-2BDlvTwjM-3D&lt=759&evt=pageLoad&sv=1&rn=152034

116. The Bing GET request above includes the same temporary and session IDs (mid, sid, vid) as the Portal page (yellow highlight), an indication that the page loaded (green highlight), information about the browser and device (grey highlight) and the same hash (pi) as the Portal (pink highlight), which identifies the computing device and allows for long term tracking. The GET request also transmitted to Bing, the URL of the page (blue highlight), which in this case also includes the fact that Plaintiff had a shoulder X-ray. This data can be used to better target ads.

117. Doubleclick's (and Google.com which was essentially similar) GET request from the test results page was:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1682104687968&cv=11&fst=1682104687968&bg=ffffff&guid=ON&async=1&gtm=45be34j0&u_w=3008&u_h=1692&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fmedical-record%2Ftest-results&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Test%20Results%20%7C%20Medical%20Record%20%7C%20Kaiser%20Permanente&auid=202926121.1682019380&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

118. The above GET request includes data about the browser and device (grey highlight) and an indication the page loaded (green highlight). The URL of the page (blue highlight) reveals Plaintiff had a shoulder X-ray. This data can be used to better target ads.

119. While Plaintiff was accessing the test results page, Google also used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je34j0&_p=1450148043&cid=1038125726.1682019380&ul=en-us&sr=3008x

1692&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&sid=1682104236&sct=2&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fva%2Finside.asp%3Fmode%3Dlabdetail%26eorderid%3D[Redacted]&dt=Search%20medical%20records&_s=1

120. The POST above includes temporary and session IDs (tid, cid, sid)—highlighted in yellow, and information about the browser and device (grey highlight). The URL of the current page (blue highlight) reveals Plaintiff's shoulder X-ray. The data sent to Google can be used to better target ads.

121. Twitter's (both analytics.twitter.com and t.co) GET request from the test results page was:

https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=06866b4e-da1b-4d15-a234-850bb5ed9e0b&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=130452a7-272c-49f6-9af1-582495f6cefc&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fsecure%2Fsearch-medical-record%3Furi%3Dsearch%253ahealth-encyclopedia%26type%3DCPT%26query%3D73030%26label%3DX%252DRAY%2BSHOULDER&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

122. The Twitter GET requests reveal in the current site URL (highlighted in blue) that plaintiff had a shoulder X-ray. This data can be used to better target ads, in this case showing a shoulder injury so that Plaintiff could be targeted for such things as shoulder slings and physical therapy services.

c) Other Searches on the Site

123. On April 20, 2023 while logged out of the Portal, Plaintiff accessed Kaiser's Health Encyclopedia and searched on Mental Health. On the search results page, Bing sent the following GET request:

https://bat.bing.com/action/0?ti=5715144&Ver=2&mid=ce46f37b-ee7d-47c6-975a-6eba4dae3726&sid=294d9520dfab11edaa7d1755dd644c7f&vid=294dbe90dfab11ed9ef7ad76fb5ac623&vids=0&msclkid=N&pi=9[Redacted]&lg=en-US&sw=3008&sh=1692&sc=24&tl=Search%20%7C%20Kaiser%20Permanente&p=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&r=https%3

A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fhealth-encyclopedia&lt=1069&evt=pageLoad&sv=1&rn=167058

124. The Bing GET request above includes temporary and session IDs (mid, sid, vid) (yellow highlight), an indication that the page loaded (green highlight), information about the browser and device (grey highlight) and the same hash (pi) as the Portal (pink highlight). The GET request also transmitted to Bing the URL of the page (blue highlight), which reveals Plaintiff's search on the term "mental health." Notably, although Plaintiff was logged out of the Portal, Bing was still able to connect the fact that Plaintiff had communicated with Kaiser Permanente about mental health because it had created a digital fingerprint. This data can be used to better target ads.

125. Doubleclick's (and Google.com which was essentially similar) GET request from the mental health search results page was:

https://googleads.g.doubleclick.net/pagead/viewthroughconversion/881418786/?random=1682019177873&cv=11&fst=1682019177873&bg=ffffff&guid=ON&async=1&gtm=45be34j0&u_w=3008&u_h=1692&url=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&ref=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fhealth-encyclopedia&label=Ump9CM7hr3IQosSlpAM&hn=www.googleadservices.com&frm=0&tiba=Search%20%7C%20Kaiser%20Permanente&auid=883163547.1682018211&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uap=macOS&uapv=13.3.1&uaw=0&data=event%3Dconversion&rfmt=3&fmt=4

126. The above GET request includes data about the browser and device (grey highlight) and an indication the page loaded (green highlight). The URL of the page (blue highlight) reveals Plaintiff searched on the term "mental health." This data can similarly be used to better target ads.

127. When Plaintiff conducted a search for "mental health", Google used the POST method to transmit the following data to Google servers at www.google-analytics.com:

https://www.google-analytics.com/g/collect?v=2&tid=G-ENXTD8TZ70&gtm=45je34j0&_p=247229106&cid=359940215.1682018211&ul=en-us&sr=3008x1692&uaa=arm&uab=64&uafvl=Chromium%3B112.0.5615.137%7CGoogle%2520Chrome%3B112.0.5615.137%7CNot%253AA-Brand%3B99.0.0.0&uamb=0&uam=&uap=macOS&uapv=13.3.1&uaw=0&_s=2&sid=1682018210&sct=1&seg=1&dl=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&dr=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fhealth-wellness%2Fhealth-encyclopedia&dt=Search%20%7C%20Kaiser%20Permanente&en=user_engagement&_et=9825

128. The POST above includes temporary and session IDs (tid, cid, sid), highlighted in yellow, and information about the browser and device (grey highlight). The URL of the current page (blue highlight) reveals Plaintiff searched for the term "mental health." The data sent to Google can be similarly be used to better target ads.

129. Twitter's (both analytics.twitter.com and t.co) GET request from the mental health search results page was:

> https://analytics.twitter.com/1/i/adsct?bci=4&eci=3&event=%7B%7D&event_id=ea2c59e7-c242-4c28-bf04-90aac0c1ab15&integration=advertiser&p_id=Twitter&p_user_id=0&pl_id=8b91e4f2-13e0-4d37-9550-913dade83cbb&tw_document_href=https%3A%2F%2Fhealthy.kaiserpermanente.org%2Fsouthern-california%2Fpages%2Fsearch%3Fquery%3Dmental%2Bhealth%26category%3Dglobal%26global-region%3Dsca%26language%3Denglish%26region%3Dsca&tw_iframe_status=0&txn_id=o2f67&type=javascript&version=2.3.29

130. The Twitter GET request in the current site URL (highlighted in blue) reveals that Plaintiff searched on the term "mental health." This data can similarly be used to better target ads.

131. On information and belief, the same type of information tracked, disclosed, and sent to Bing, Google, and Twitter for Plaintiff has been tracked, disclosed, and sent to Bing, Google, and Twitter for other members of the Classes.

132. Whenever Kaiser Plan Members use Kaiser Permanente's website, Kaiser Permanente allows Bing, Google, and Twitter to intercept the contents of their communications—including personal information, identifying information, and sensitive medical information—without their knowledge, consent, or authorization.

133. Kaiser Permanente knowingly redirects and discloses Kaiser Plan Members' personally identifiable patient data, including their status as patients and the contents of their communications with Kaiser Permanente to Bing, Google, and Twitter.

134. Despite its legal obligations to keep this information and these communications private and confidential, Kaiser Permanente's use of Bing, Google, and Twitter analytics causes the redirection, interception, and transmission of the precise content of patients' communication with Kaiser Permanente to Bing, Google, and Twitter.

135. Kaiser Permanente's unauthorized redirection and disclosures to Bing, Google, and Twitter includes information that identifies Plaintiff and Class Members as patients of Kaiser

Permanente, and aids in receiving and recording patient communications pertaining to or about specific medical conditions, health services, and specific doctors.

136. Kaiser Permanente's disclosures to Bing, Google, and Twitter occur because Kaiser Permanente intentionally deploys Bing, Google, and Twitter code on its website, and that code commandeers Kaiser Plan Members' web-browsers and causes personally identifiable patient data, as well as the contents of communications exchanged between Kaiser Permanente and its patients, to be redirected and sent to Bing, Google, and Twitter.

137. As currently deployed, Bing, Google, and Twitter analytics, as employed by Kaiser Permanente, functions as a wiretap, and Bing, Google, and Twitter as third-party wiretappers.

C. Plaintiff and Class Members Did Not Consent to Kaiser Permanente Disclosure of Their Information and Communications to Third Parties

138. Kaiser Permanente does not ask Kaiser Plan Members who use its Site and Portal, including Plaintiff, whether they consent to having the contents of their information and communications with Kaiser Permanente disclosed to the Third Party Wiretappers. Kaiser Plan Members are never actively told that their electronic communications are being wiretapped by Third Party Wiretappers.

139. Kaiser Permanente states in its Privacy Policy, under the heading "Internet Cookies," that:

> We and our service providers *may* place Internet "cookies" or similar technologies (JavaScript, HTML5, ETag) on the computer hard drives of visitors to the Site. Information we obtain helps us to tailor our Site to be more helpful and efficient for our visitors. For example, we are able to see the navigation path taken by users, and that information allows us to understand user success or challenges with the web experience. *The cookie consists of a unique identifier that does not contain information about your health history*. We use two types of cookies, 'session' cookies and "persistent" cookies, along with other similar technologies.

Website and mobile application Privacy Statement, Kaiser, https://healthy.kaiserpermanente.org /privacy (last visited May 3, 2023) (emphasis added).

140. This does not disclose that Kaiser Permanente sends Plaintiff's and Class Members' information and communications to the Third Party Wiretappers.

141. First, these "third parties" are not defined in the Website Privacy Policy.

142. Second, disclosing that others *may* monitor certain information is not the same as disclosing that others *do in fact* collect user data in real time.

143. Third, Kaiser Permanente falsely claims that information about Kaiser Plan Members' health history is not being transmitted.

144. Fourth, alerting users to the possible use of "cookies . . . and other tracking technologies" does not put Kaiser Plan Members on notice of the use of technology like Session Replay, and other technology used by the Third Party Wiretappers, which, unlike first party cookies, (1) communicate information to an external server as a user navigates a website; (2) track users across devices; (3) are not easily disabled by users; and/or (4) essentially creates a recording of all the information that visitors provide or receive from Kaiser Permanente on the Site.

145. Fifth, disclosures to the Third Party Wiretappers are not made only for the purpose of tailoring the Kaiser Permanente website to be more helpful and efficient for Kaiser Plan Members who use the Site and Portal, but is instead used for marketing purposes, including to produce targeted advertising for third parties.

D. Plaintiff's and Class Members' Health Information Has Actual, Measurable, Monetary Value

146. Kaiser Plan Members' confidential communications and information that Kaiser Permanente allows the Third Party Wiretappers to intercept has monetary value.

147. For example, one recent study asked over a thousand consumers from around the world what price they would demand of third parties for access to their data and found that passwords would fetch $75.80; health information and medical records themselves average $59.80; and in third, Social Security numbers were valued at $55.70.[29]

148. Some companies, such as Prognos Health, sell what they purport to be de-identified health information from millions of patients.[30]

[29] Jonathan Weicher, *Healthcare hacks—how much is your personal information worth?*, Netlib Security, https://netlibsecurity.com/articles/healthcare-hacks-how-much-is-your-personal-information-worth/ (last visited Apr. 28, 2023).

[30] Press Release, *Prognos Health Announces Patent-Pending Technology* (Apr. 6, 2021), https://prognoshealth.com/about-us/news/press-release/prognos-health-announces-patent-pending-technology.

149. Due to the difficulty in obtaining health information, illegal markets also exist for such data, with some reporting that health data can be "more expensive than stolen credit card numbers."[31]

E. Kaiser Permanente's Conduct Violates State and Federal Privacy Laws

150. Kaiser Plan Members have a reasonable expectation of privacy in their identifying information, personal and sensitive medical information and communications with Kaiser Permanente and its providers, rooted in state and federal privacy laws as well as Kaiser Permanente's express and implied contracts and disclosures. This includes a reasonable expectation that Kaiser Plan Members' identifying information, personal and sensitive medical information and communications with Kaiser Permanente and its providers will not be disclosed to or tracked by Third Party Wiretappers and will not be disclosed to third parties for marketing purposes.

151. Plaintiff and Class Members reasonably believed their interactions with Kaiser Permanente on the Site and Portal were private and would not be transmitted to third parties, recorded, or monitored for a later playback.

152. The data collected by Kaiser Permanente identified specific web pages navigated and content viewed, and thus revealed personalized and sensitive information about Plaintiff and Class Members, including sensitive personal and medical information.

153. Plaintiff and Class Members did not have a reasonable opportunity to discover Defendants' unlawful and unauthorized connections and conduct because Kaiser Permanente did not disclose its actions nor seek consent from Plaintiff or Class Members prior to making the transmissions to third parties.

154. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares its customers' personal data.

[31] Aarti Shahani, *The Black Market For Stolen Health Care Data*, NPR (Feb. 13, 2015, 4:55 am), https://www.npr.org/sections/alltechconsidered/2015/02/13/385901377/the-black-market-for-stolen-health-care-data.

155. For example, a study by Pew Research Center indicated that an overwhelming majority of Americans—approximately 79%—are concerned about how data is collected about them by companies.[32]

156. As Kaiser Plan Members, Plaintiff and Class Members have a reasonable expectation of privacy that Kaiser Permanente, their health care provider, will not disclose the content of their personal and medical information and confidential communications with Kaiser Permanente and its providers to third parties without their express authorization.

157. Plaintiff's and Class Members' reasonable expectation of privacy in their personally identifiable data and communications exchanged with Kaiser Permanente and its providers is derived from several sources, including:

a. Kaiser Permanente's status as Kaiser Plan Members' health care provider;

b. Kaiser Permanente's common law obligation to maintain confidentiality of patient data and communications;

c. State and federal laws and regulations protecting the confidentiality of medical information;

d. State and federal laws protecting the confidentiality of communication and computer data;

e. Defendants' express promises of privacy and confidentiality; and

f. Defendants' implied promises of privacy and confidentiality.

158. Significantly, patient health care data in the United States is protected by federal law under HIPAA and its implementing regulations, which are promulgated by the HHS.

159. The HIPAA Privacy Rule, located at 45 CFR § 160 and Subparts A and E of § 164, "establishes national standards to protect individuals' medical records and other individually identifiable health information (collectively defined as 'protected health information') and applies to

[32] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[33]

160. The Privacy Rule broadly defines "protected health information" ("PHI") as "individually identifiable health information" ("IIHI") that is "(i) [t]ransmitted by electronic media; (ii) [m]aintained in electronic media; or (iii) [t]ransmitted or maintained in any other form or medium." 45 C.F.R. § 160.103.

161. IIHI is defined as "a subset of health information, including demographic information collected from an individual" that is: (1) "created or received by a health care provider, health plan, employer, or health care clearinghouse"; (2) "[r]elates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual"; and (3) either (a) "identifies the individual" or (b) "[w]ith respect to which there is a reasonable basis to believe the information can be used to identify the individual." 45 C.F.R. § 160.103.

162. The HIPAA Privacy Rule requires any "covered entity"—which includes health care providers—to maintain appropriate safeguards to protect the privacy of protected health information and sets limits and conditions on the uses and disclosures that may be made of protected health information without authorization. 45 C.F.R. §§ § 160.103, 164.502.

163. An individual or corporation violates the HIPAA Privacy Rule if it knowingly: "(1) uses or causes to be used a unique health identifier; [or] (2) obtains individually identifiable health information relating to an individual." 42 U.S.C. § 1320d-6. The statute states that a "person . . . shall be considered to have obtained or disclosed individually identifiable health information . . . if the information is maintained by a covered entity . . . and the individual obtained or disclosed such information without authorization." *Id.*

164. The criminal and civil penalties imposed by 42 U.S.C. § 1320d-6 apply directly to Kaiser Permanente when it knowingly disclosed individually identifiable health information relating to an individual, as those terms are defined under HIPAA.

[33] *The HIPAA Privacy Rule*, HHS, https://www.hhs.gov/hipaa/for-professionals/privacy/index.html (last visited Apr. 28, 2023).

165. Violation of 42 U.S.C. § 1320d-6 is subject to criminal penalties. 42 U.S.C. § 1320d-6(b). There is a penalty enhancement where "the offense is committed with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm." *Id.* In such cases, the entity that knowingly obtains individually identifiable health information relating to an individual shall "be fined not more than $250,000, imprisoned not more than 10 years, or both." *Id.*

166. Guidance from HHS confirms that patient status is protected by HIPAA, which provides

> Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book, then this information would not be PHI because it is not related to health data. . . . ***If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.***[34]

167. HHS' guidance for marketing communications states that health care providers may not provide patient lists for marketing purposes without the consent of every included patient:

> The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. . . . Simply put, a covered entity may not sell protected health information to a business associate or any other third party for that party's own purposes. **Moreover, covered entities may not sell lists of patients or enrollees to third parties without obtaining authorization from each person on the list**.[35]

168. HHS has previously instructed that patient status is protected by the HIPAA Privacy Rule:

> a. "[T]he sale of a patient list to a marketing firm" is not permitted under HIPAA. 65 Fed. Reg. 82717 (Dec. 28, 2000);
>
> b. "[A] covered entity must have the individual's prior written authorization to use or disclose protected health information for marketing communications," which

[34] *Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule* at 5 (Nov. 26, 2012), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/Deidentification/hhs_deid_guidance.pdf. (emphasis added) (last visited Apr. 28, 2023).

[35] *Marketing* at 1-2, Office for Civil Rights (Rev. Apr. 3, 2003), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/marketing.pdf. (emphasis added).

includes disclosure of mere patient status through a patient list. 67 Fed. Reg. 53186 (Aug. 14, 2002);

c. It would be a HIPAA violation "if a covered entity impermissibly disclosed a list of patient names, addresses, and hospital identification numbers." 78 Fed. Reg. 5642 (Jan. 25, 2013); and

d. The only exception permitting a hospital to identify patient status without express written authorization is to "maintain a directory of individuals in its facility" that includes name, location, general condition, and religious affiliation when used or disclosed to "members of the clergy" or "other persons who ask for the individual by name." 45 C.F.R. § 164.510(1). Even then, patients must be provided an opportunity to object to the disclosure of the fact that they are a patient. 45 C.F.R. § 164.510(2).

V. TOLLING

169. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

170. The statutes of limitations applicable to Plaintiff's and the Classes' claims were tolled by Defendants' conduct and Plaintiff's and Class Members' delayed discovery of their claims.

171. As alleged above, Plaintiff and members of the Classes did not know and could not have known when they used the Kaiser Permanente Site and/or Portal that Kaiser Permanente was disclosing their information and communications to third parties. Plaintiff and members of the Classes could not have discovered Kaiser Permanente's unlawful conduct with reasonable diligence.

172. Kaiser Permanente secretly incorporated the Third Party Wiretappers' code into the Site, including the Portal, providing no indication to Kaiser Plan Members and Site users that their communications would be disclosed to these third parties.

173. Kaiser Permanente had exclusive and superior knowledge that the Third Party Wiretappers' code incorporated on its Site would disclose Kaiser Plan Members' protected and private information and confidential communications, yet failed to disclose to Kaiser Plan Members and Site users that by interacting with the Kaiser Permanente Site and/or Portal that Plaintiff's and Class Members' patient status, personal information, sensitive health information, and confidential communications would be disclosed to third parties.

174. Plaintiff and Members of the Classes could not with due diligence have discovered the full scope of Kaiser Permanente's conduct because the incorporation of the Third Party Wiretappers' code is highly technical and there were no disclosures or other indication that would inform a

reasonable consumer or Site user that Kaiser Permanente was disclosing and allowing the interception of such information to these third parties.

175. The earliest Plaintiff and Class Members could have known about Defendants' conduct was shortly before the filing of this Complaint.

VI. CLASS ACTION ALLEGATIONS

176. Plaintiff brings this action pursuant to Federal Rules of Civil Procedure 23(a) and 23(b)(2) and/or (b)(3) on behalf of the following Class and Sub-Classes:

> **Nationwide Class:** All Kaiser Plan Members in the United States who used the Kaiser Permanente website.
>
> **California Sub-Class:** All Kaiser Plan Members who are residents of the State of California and used the Kaiser Permanente website.
>
> **Nationwide Breach of Contract Sub-Class:** All Kaiser Plan Members who used the Portal on the Kaiser Permanente website.
>
> **California Breach of Contract Sub-Class**: All Kaiser Plan Members who are residents of the State of California and used the Portal on the Kaiser Permanente website.

177. Excluded from the Class and Sub-Class are Defendants and their parents, subsidiaries, and corporate affiliates. Plaintiff reserves the right to revise the definition of the Class and Sub-Class based upon subsequently discovered information and reserves the right to establish additional Sub-Class where appropriate. The Class and Sub-Class are collectively referred to herein as the "Class" or "Classes."

178. The Classes are so numerous that joinder of all members is impracticable. Plaintiff believes that there are at least tens of thousands of proposed members of the Classes throughout the United States.

179. Common questions of law and fact exist as to all members of the Class and predominate over any issues solely affecting individual members of the Class. The common and predominating questions of law and fact include, but are not limited to:

- Whether Defendants' acts and practices violated the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*;
- Whether Defendants' acts and practices violated the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*;

- Whether Defendants' acts and practices violated California's Constitution, Art. 1, § 1;
- Whether Defendants' acts and practices violations Plaintiff's and Class Members' common law privacy rights;
- Whether Defendants breached a express contract;
- Whether Defendants breached an implied contract; and
- Whether damages, restitution, equitable, injunctive, compulsory, or other relief is warranted.

180. Plaintiff's claims are typical of the claims of the Class that Plaintiff seeks to represent. As alleged herein, Plaintiff and the Class sustained damages arising out of the same unlawful actions and conduct by Defendants.

181. Plaintiff is willing and prepared to serve the Class in a representative capacity with all of the obligations and duties material thereto. Plaintiff will fairly and adequately protect the interests of the Class and has no interest adverse to or in conflict with the interests of the other members of the Class.

182. Plaintiff's interests are co-extensive with and are not antagonistic to those of absent members within the Class. Plaintiff will undertake to represent and protect the interests of absent members within the Class and will vigorously prosecute this action.

183. Plaintiff has engaged the services of the undersigned counsel. Counsel is experienced in complex litigation, will adequately prosecute this action and will assert and protect the rights of, and otherwise represent, Plaintiff and absent members of the Class.

184. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Plaintiff knows of no difficulty to be encountered in the management of this litigation that would preclude its maintenance as a class action.

185. Class action status is warranted under Federal Rule of Civil Procedure 23(b)(3) because questions of law or fact common to the members of the Classes predominate over any questions affecting only individual members, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

186. The Class may also be certified under Federal Rule of Civil Procedure 23(b)(2) because Defendants have acted on grounds generally applicable to the Classes, thereby making it

appropriate to award final injunctive relief or corresponding declaratory relief with respect to the Classes.

187. The interest of members within the Class individually controlling the prosecution of separate actions is theoretical and not practical. The Classes have a high degree of similarity and are cohesive, and Plaintiff anticipates no difficulty in the management of this matter as a class action.

188. The nature of notice to the proposed Class is contemplated to be by direct mail and/or email upon certification of the Class or, if such notice is not practicable, by the best notice practicable under the circumstance including, *inter alia*, email, publication in major newspapers, and/or on the internet.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
Violation of the Electronic Communications Privacy Act, 18 U.S.C §§ 2510, *et seq.*
(On Behalf of the Nationwide Class)

189. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

190. Plaintiff brings this claim individually and on behalf of the Nationwide Class.

191. The Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510, *et seq*., prohibits the interception of any wire, oral, or electronic communications without the consent of at least one authorized party to the communication.

192. The ECPA confers a civil cause of action on "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter." 18 U.S.C. § 2520(a).

193. The ECPA protects both the sending and receipt of communications.

194. A violation of the ECPA occurs where any person "intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any . . . electronic communication" or "intentionally discloses, or endeavors to disclose, to any other person the contents of any . . . electronic communication, knowing or having reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication" or "intentionally uses, or endeavors to use, the contents of any . . . electronic communication, knowing or having

reason to know that the information was obtained through the [unlawful] interception of a[n] . . . electronic communication." 18 U.S.C. §§ 2511(1)(a), (c)-(d).

195. In addition, "a person or entity providing an electronic communication service to the public shall not intentionally divulge the contents of any communication . . . while in transmission on that service to any person or entity other than an addressee or intended recipient of such communication or an agent of such addressee or intended recipient." 18 U.S.C. § 2511(3)(a).

196. "Intercept" means "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4).

197. "Electronic communication" means "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce." 18 U.S.C. § 2510(12).

198. "Contents" includes "any information concerning the substance, purport, or meaning" of the communication at issue. 18 U.S.C. § 2510(8).

199. An "electronic communication service" means "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15).

200. Plaintiff and Nationwide Class Members' communications with Kaiser Permanente through the Site, including the Portal, are electronic communications under the ECPA.

201. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser Permanente and/or their health care providers on the Site, Third Party Wiretappers, through the source code Kaiser Permanente embedded and ran on its website, contemporaneously and intentionally intercepted, and endeavored to intercept Plaintiff's and Nationwide Class Members' electronic communications without authorization or consent.

202. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source code it imbedded and ran on its website, contemporaneously and intentionally disclosed, and

endeavored to disclose the contents of Plaintiff's and Nationwide Class Members' electronic communications to the Third Party Wiretappers, without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

203. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source code it embedded and ran on the Site, contemporaneously and intentionally used, and endeavored to use and allow the contents of Plaintiff's and Nationwide Class Members' electronic communications to be disclosed and used for purposes other than providing health care services to Plaintiff and Nationwide Class Members without authorization or consent, and knowing or having reason to know that the electronic communications were obtained in violation of the ECPA.

204. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source code it embedded and ran on the Site, contemporaneously and intentionally redirected the contents of Plaintiff's and Nationwide Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, namely the Third Party Wiretappers.

205. Whenever Plaintiff and Nationwide Class Members communicated with Kaiser Permanente and/or their health care providers on the Site, Kaiser Permanente, through the source code it embedded and ran on the Site, contemporaneously and intentionally divulged the contents of Plaintiff's and Nationwide Class Members' electronic communications while those communications were in transmission, to persons or entities other than an addressee or intended recipient of such communication, namely the Third Party Wiretappers.

206. The Third Party Wiretappers intentionally intercepted and used the contents of Plaintiff's and Nationwide Class Members' electronic communications for the unauthorized purpose of profiting from Plaintiff's and Nationwide Class Members' communications, including by generating advertising revenue.

207. Plaintiff and Nationwide Class Members did not authorize Kaiser Permanente to disclose the content of their communications with Kaiser Permanente to the Third Party Wiretappers.

208. Plaintiff and Nationwide Class Members did not authorize the Defendants' interception, redirection, disclosure, and/or use of their sensitive, private health information and communications in their electronic communications with Kaiser Permanente. The Third Party Wiretappers are not party to these communications.

209. Because the interception of Plaintiff's and Nationwide Class Members' communications was without authorization and consent from Plaintiff and Nationwide Class Members, and included confidential information protected under HIPAA, the interception was unlawful, tortious, and/or constituted a criminal act.

210. Defendants' actions were at all relevant times knowing, willful, and intentional.

211. Pursuant to 18 U.S.C. § 2520, Plaintiff and Nationwide Class Members have been damaged by the interception, disclosure, and/or use of their communications in violation of the ECPA and are entitled to: (1) appropriate equitable or declaratory relief; (2) damages, in an amount to be determined at trial, assessed as the greater of (a) the sum of the actual damages suffered by Plaintiff and the Class and any profits made as a result of the violation, or (b) statutory damages of whichever is the greater of $100 per day per violation or $10,000; and (3) reasonable attorneys' fees and other litigation costs reasonably incurred.

SECOND CLAIM FOR RELIEF
Violation of the California Invasion of Privacy Act
Cal. Penal Code §§ 630, *et seq.* ("CIPA")
(On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class)

212. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

213. Plaintiff brings this claim individually and on behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class.

214. The California Legislature enacted the California Invasion of Privacy Act, Cal. Penal Code §§ 630, *et seq.*, to address "advances in science and technology [that] have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of

such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.* § 630. CIPA is intended "to protect the right of privacy of the people of this state." *Id.*

215. To establish liability under section 631(a), Plaintiff need only establish that a Defendant, "by means of any machine, instrument, or contrivance, or in any other manner," did any of the following:

> [i] [I]ntentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system,
>
> Or
>
> [ii] [W]illfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state,
>
> Or
>
> [iii] [U]ses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained,
>
> Or
>
> [iv] [A]ids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

216. Under § 631, a defendant must show it had the consent of all parties to a communication.

217. Kaiser Permanente and the Third Party Wiretappers are each a "person" for the purposes of CIPA.

218. Defendants maintain their headquarters in California, where they designed, contrived, agreed, conspired, effectuated, aided, and/or received the interception and use of the contents of Plaintiff and Class Members' communications.

219. The Third Party Wiretappers' code, Quantum Metric's recording code, Plaintiff's and Class Members' browsers and Plaintiff's and Class Members' computing and mobile devices are all a "machine, instrument, or contrivance, or . . . other manner" used to engaged in the prohibited conduct at issue here. Cal. Penal Code § 631.

220. Kaiser Permanente installed the Third Party Wiretappers' code to automatically and secretly spy on, and intercept Plaintiff's and Class Members' communications with Kaiser Permanente through the Kaiser Permanente website in real time.

221. At all relevant times, Kaiser Permanente's disclosure of Plaintiff and Class Members' internet communications to Third Party Wiretappers was without Plaintiff and Class Members' authorization or consent.

222. By installing the Third Party Wiretappers' code on its website, Kaiser Permanente intentionally caused Plaintiff and Class Members' communications to be intercepted, recorded, stored, and transmitted to the Third Party Wiretappers.

223. At all relevant times, the Third Party Wiretappers intentionally tapped or made unauthorized connections with, the lines of internet communication between Plaintiff and Class Members and Kaiser Permanente's Site without the consent of all parties to the communication.

224. The Third Party Wiretappers willfully read or attempt to read or learn the contents or meaning of Plaintiff and Class Members' communications to Kaiser Permanente's Site while the communications are in transit or passing over any wire, line, or cable, or were being received at any place within California when it intercepted Plaintiff's and Class Members' communications with Kaiser Permanente's Site in real time.

225. By embedding the Third Party Wiretappers' technology on its website, Kaiser Permanente aided, agreed with, employed, and conspired with Third Party Wiretappers to carry out the wrongful conduct alleged herein in violation of Cal. Penal Code § 631(a)[iv].

226. Plaintiff and the Class Members seek statutory damages in accordance with § 637.2(a), which provides for the greater of: (1) $5,000 per violation; or (2) three times the amount of damages sustained by Plaintiff and the Class in an amount to be proven at trial, as well as injunctive or other equitable relief.

THIRD CLAIM FOR RELIEF
Common Law Invasion of Privacy—Intrusion Upon Seclusion
(On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class)

227. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

228. Plaintiff brings this claim individually and on behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class.

229. Intrusion upon seclusion has occurred when (1) Defendants intruded and/or aided, agreed with, employed, and/or conspired with the Third Party Wiretappers to intrude into a private place, conversation, matter; (2) in a manner was highly offensive to a reasonable person.

230. Kaiser Permanente intentionally intruded upon Plaintiff and Class Members' solitude or seclusion when it disclosed communications it received from Plaintiff and Class Members, which was intended to stay private, to Third Party Wiretappers.

231. Plaintiff and Class Members did not consent to or authorize, nor were they aware of (1) Kaiser Permanente's disclosure to Third Party Wiretappers of information that it received from Plaintiff and Class Members through its Site or (2) the Third Party Wiretappers' collection of information concerning Plaintiff and Class Members' activity on the Kaiser Permanente website at the time that the disclosure occurred. Plaintiff and Class Members never agreed that Kaiser Permanente could disclose their communications to Third Party Wiretappers, nor did they agree that the Third Party Wiretappers could collect such information.

232. Plaintiff and Class Members had a reasonable expectation of privacy over their communications with Kaiser Permanente, including information obtained from their use of Kaiser Permanente's Site, including the Portal.

233. Kaiser Permanente's and the Third Party Wiretappers' intentional intrusion into Plaintiff and Class Member's communications with Kaiser Permanente, including information obtained from their use of Kaiser Permanente's Site, was highly offensive to a reasonable person in that it violated federal and state criminal and civil laws designed to protect individual privacy.

234. The disclosure and collection of communications with Kaiser Permanente, including information obtained from their use of Kaiser Permanente's Site through deceit is highly offensive to a reasonable person. Plaintiff and Class Members reasonably expected that their communications with Kaiser Permanente, including information obtained from their use of Kaiser Permanente's Site would not be disclosed to third parties.

235. Secret disclosure and collection of Plaintiff's and Class Members' communications with Kaiser Permanente, including information of thousands of individuals obtained from their use of Kaiser Permanente's Site is highly offensive to a reasonable person. Privacy polls and studies show that the overwhelming majority of Americans believe one of the most important privacy rights is the need for an individual's affirmative consent before personal information is collected or shared.

236. Plaintiff and Class Members have suffered harm and injury as a direct and proximate result of Kaiser Permanente's invasion of their privacy.

237. Plaintiff and Class Members are entitled to reasonable compensation, including but not limited to monetary damages.

238. Plaintiff and Class Members seek appropriate relief for that injury, including, but not limited to injunctive relief and damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of its intrusions upon Plaintiff's and Class Members' privacy.

239. Plaintiff also seeks such other relief as the Court may deem just and proper.

FOURTH CLAIM FOR RELIEF
Invasion of Privacy and Violation of the California Constitution, Art. 1, § 1
(On Behalf of the Nationwide Class, or alternatively, On Behalf of the California Sub-Class)

240. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

241. Plaintiff brings this claim individually and on behalf of the Nationwide Class, or alternatively, on behalf of the California Sub-Class.

242. Kaiser Permanente is headquartered in California and its conduct took place in California.

243. Article I, section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy." Cal. Cons. art. I, § 1.

244. The right to privacy in California's constitution creates a right of action against private entities such as Kaiser Permanente.

245. To state a California constitutional privacy claim, a plaintiff must establish (1) a legally protected privacy interest; (2) where the plaintiff had a reasonable expectation of privacy; and (3) conduct by the defendant constituting an intrusion of privacy so serious in nature, scope, and actual or potential impact as to constitute an egregious breach of the social norms.

246. Plaintiff and Class Members possess a legally protected interest in their communications with Kaiser Permanente, including information derived from their use of Kaiser Permanente's Site, and in providing such information to Kaiser (and receiving information from Kaiser Permanente) without that information being disclosed to Third Party Wiretappers. This legally-protected interest is derived from the common law, the California Constitution's article I, section 1 guarantee of the right to privacy, the ECPA, CIPA, and HIPAA.

247. Plaintiff and Class Members had a reasonable expectation of privacy under the circumstances, including that: (i) the information Kaiser Permanente disclosed to Third Party Wiretappers included information related to patient status, health conditions, identifying information, personal and sensitive information, information related to medical treatment, and confidential communications with Kaiser Permanente and its providers; and (ii) Plaintiff and Class Members did not consent or otherwise authorize Kaiser Permanente to disclose this private information and these confidential communications to the Third Party Wiretappers.

248. Defendants' conduct constituted a serious invasion of privacy that would be highly offensive to a reasonable person in that: (i) the information disclosed by Kaiser Permanente and collected by Third Party Wiretappers was highly sensitive and personal, as protected by the California Constitution; (ii) Kaiser Permanente did not have authorization or consent to disclose this information to any third party, including Third Party Wiretappers, and the Third Party Wiretappers did not have authorization to collect this information; and (iii) the invasion deprived Plaintiff and Class Members the ability to control the circulation of said information, which is considered a fundamental right to privacy.

249. Defendants' invasion violated the privacy rights of thousands of Class Members, including Plaintiff, without authorization or consent. Their conduct constitutes a severe and egregious breach of social norms.

250. As a direct and proximate result of Defendants' actions, Plaintiff and Class Members have had their privacy invaded and sustained damages and will continue to suffer damages.

251. Plaintiff and Class Members seek appropriate relief for that injury, including but not limited to injunctive relief and damages that will reasonably compensate Plaintiff and Class Members for the harm to their privacy interests as well as a disgorgement of profits earned as a result of their intrusions upon Plaintiff's and Class Members' privacy.

252. Plaintiff also seeks such other relief as the Court may deem just and proper.

FIFTH CAUSE OF ACTION
Breach of Express Contract
(On Behalf of the Nationwide Breach of Contract Sub-Class or alternatively, On Behalf of the California Breach of Contract Sub-Class)

253. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

254. Plaintiff brings this claim individually and on behalf of the Nationwide Breach of Contract Class, or alternatively, on behalf of the California Breach of Contract Sub-Class.

255. There exists an express contract between Plaintiff and Breach of Contract Class Members on the one side, and Kaiser Permanente on the other, when Plaintiff and Breach of Contract Class Members accessed information on the Kaiser Permanente Portal, namely the Terms and Conditions and Privacy Policy for the Kaiser Permanente website (hereinafter referred to as the "express contract" or "Site Terms and Conditions"). A true and correct copy of the Site Terms and Conditions[36] currently in effect is attached hereto as Exhibit 1, and a copy of the Privacy Statement, incorporated into the Terms and Conditions, is attached as Exhibit 2.

256. Specifically, at the bottom of the Portal Login Page, Kaiser Permanente agrees, contracts, and warrants that: "By signing in, you agree to our website Terms & Conditions and Privacy Statement." https://healthy.kaiserpermanente.org/southern-california/register (last visited May 3, 2023).

[36] The Terms and Conditions are materially identical for all Kaiser Permanente Regions.

257. The Kaiser Permanente Terms & Conditions, available via hyperlink, provides: "Any personal information you submit to the Site (for yourself or someone else) is governed by our Website and KP Mobile Application Privacy Statement." *Terms & Conditions for our Website and Mobile Application*, *supra* note 3.

258. In the Kaiser Permanente Privacy Statement, also available via hyperlink, Kaiser Permanente also agrees, contracts, and warrants that Kaiser Permanente's data collection "is collected on an aggregate basis, which means that no personally identifiable information is associated with the data."

259. In the Kaiser Permanente Privacy Statement, Kaiser Permanente states that Kaiser Permanente and its service providers may place "cookies" or similar technologies on the computer hard drives of visitors to the Site, and further agrees, contracts, and warrants that information obtained from cookies is only used to help Kaiser Permanente "tailor our Site to be more helpful and efficient for our visitors."

260. In the Kaiser Permanente Privacy Statement, Kaiser Permanente agrees, contracts, and warrants that "[t]he cookie consists of a unique identifier that does not contain information about your health history."

261. The Kaiser Permanente Privacy Statement also states that Kaiser "may also occasionally use 'Web beacons' (also known as 'clear gifs,' 'Web bugs,' '1-pixel gifs,' etc.)" and Kaiser Permanente also agrees, contracts, and warrants that Kaiser Permanente Kaiser will "not collect any personal health information" through this technology.

262. Kaiser Permanente then makes the following promises in the Privacy Statement, which is incorporated as part of the express contract:

- "Use and disclosure of health information includes using the information to provide treatment to the individual, to make payments for such treatment, and to conduct ongoing quality improvement activities. Our use and disclosure of an individual's personal information (including health information) is limited as required by state and federal law."
- "In addition to web logs, described below, Kaiser Permanente routinely gathers data on Site activity, such as how many people visit the Site, the web pages or mobile screens they visit, where they come from, how long they stay, etc. ***The data is collected on an aggregate basis, which means that no personally identifiable information is associated with the data.*** This data helps us improve our content

> and overall usage. The information is not shared with other organizations for their independent use." (emphasis added).

263. In addition, Kaiser promises that "we do not collect any personally identifiable information about visitors to the Site. The policies, sources, uses and disclosures of information are outlined in Sections 1 through 20 that follow."

264. Sections 2, 3, and 4 address "Web logs," "Internet cookies," and "Web Beacons," however, neither section describes the extensive information collection to which patient information is subjected by the Kaiser website.

265. The Kaiser Permanente Privacy Statement does not disclose to Kaiser Plan Members that Kaiser Permanente has aided, agreed with, employed, and/or conspired with third parties that are recording all of the information that Kaiser Plan Members' are sending, accessing, reviewing, or receiving through the Site.

266. These terms create a contractual relationship between Kaiser Permanente and any patient to whom it gives access to the Portal, including Plaintiff and Breach of Contract Class Members.

267. Despite its assurances of privacy and confidentiality, Kaiser Permanente intentionally incorporated the Third Party Wiretappers' code and recording technology on the Kaiser Permanente Site, including the Portal, disclosing the contents of Plaintiff and Breach of Contract Class Members' information and confidential communications with Kaiser Permanente and its providers to Third Party Wiretappers, including for advertising purposes.

268. In exchange for Kaiser Permanente's provision of a secure website and patient Portal, Plaintiff and Breach of Contract Class Members were able to make appointments, view medical history, get test results, and find and communicate with doctors, among other things, by way of the patient Portal, instead of doing so by other means, such as by phone or in person.

Consent

269. Kaiser Permanente requires Kaiser Plan Members to consent to the Site Terms and Conditions in the process of signing up for, and using, the patient Portal.

270. Plaintiff John Doe and Breach of Contract Class Members consented to the Site Terms and Conditions by signing up for, and using, the Kaiser Permanente patient Portal.

Consideration

271. The Kaiser Permanente patient Portal is not a service Kaiser provides without receiving anything from Plaintiff and Breach of Contract Class Members in return. To the contrary, Plaintiff's and Breach of Contract Class Members' use of the patient Portal confers significant benefit upon Kaiser Permanente—a benefit to which Kaiser Permanente is not entitled—including, but not limited to, increased efficiency, optimized workflow, cost reduction, and receipt of incentive payments from the federal government (HHS) via the Meaningful Use Program. As just one example, Breach of Contract Class Members use of the patient Portal, to access test results and make appointments, results in Kaiser Permanente being freed up from performing such tasks of scheduling and reporting on test results for patients, thereby cutting down on long phone calls or in-office communications, increasing efficiency and decreasing costs.

272. In fact, according to a blog post on the health policy website, Health Affairs,[37] Kaiser Permanente offers "the largest private-sector patient portal in the U.S.," which "help[s] our health care system improve outcomes and manage resources." The Portal has led to a "2 to 6.5 percent improvement in Healthcare Effectiveness Data and Information Set (HEDIS) performance measures," improved patient loyalty by making portal uses "2.6 times more likely to remain Kaiser Permanente members," and shifted patient interactions from in-person to secure messenger.

273. Thus, Kaiser Permanente benefits from Breach of Contract Class Members' use of their online Portal by: (1) making their provision of healthcare services more efficient, and (2) reducing the costs associated with managing their members' medical conditions. Importantly, as an integrated managed care consortium, Kaiser Permanente is both a healthcare provider and insurer—thus, they are in a position to realize any savings generated by reducing patient costs.

[37] Terhilda Garrido, Brian Raymond, & Ben Wheatley, *Lessons From More Than A Decade In Patient Portals*, Health Affairs (Apr. 7, 2016), https://www.healthaffairs.org/do/10.1377/forefront.20160407.054362.

Performance

274. Plaintiff John Doe and Breach of Contract Class Members performed under the express contract.

Kaiser Permanente's Breach of the Express Contract

275. Kaiser Permanente materially breached its express contract with Plaintiff and Breach of Contract Class Members by disclosing to the Third Party Wiretappers, Plaintiff's and Breach of Contract Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente, thereby failing to provide Plaintiff and Breach of Contract Class Members with the secure method of communication it agreed to provide.

276. The patient health information Kaiser Permanente used and disclosed to unauthorized third parties includes:

a. Breach of Contract Class Members' IP addresses, User-Agent data, persistent cookie identifiers, device identifiers, and/or browser fingerprint information—all of which constitute personally identifiable data both alone and in combination with other data;

b. the date and time of Breach of Contract Class Members' registration for the Portal;

c. the date and time of every Breach of Contract Class Members' sign-in and logoff of the "secure" the Portal;

d. the contents of communications Breach of Contract Class Members' exchange inside the "secure" Portal;

e. the contents of communications Breach of Contract Class Members' exchange after they have logged off the Portal;

f. the contents of communications Breach of Contract Class Members' exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the "secure" Portal; and

g. all other HTTPS communications patients exchange with Kaiser Permanente and its providers on the Site that Kaiser Permanente has permitted the third parties to correlate with the patient's status as a patient, and the particular dates and times

for which they access the "secure" Portal.

277. The patient data Kaiser Permanente discloses (Plaintiff's and Breach of Contract Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente and its providers) is not aggregated as specified in the Privacy Statement.

278. Nevertheless, information that Plaintiff and Breach of Contract Class Members reasonably thought was being transmitted "securely" to Kaiser Permanente was being disclosed by Kaiser Permanente to unauthorized third parties as follows:

a. A Kaiser Plan Member signs in to the "secure" patient Portal;

b. On sign-in, Kaiser Permanente discloses the fact of the sign in to Adobe, Bing, Google, Quantum Metric, and Twitter;

c. Once signed-in, if a Kaiser Plan Member clicked to, for example:

i. view tests, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter of the specific tests; or,

ii. Find-A-Doctor, or set an appointment, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter.

d. The above examples of patient communications about the doctor or the appointment was shared with Adobe, Bing, Google, Quantum Metric, and Twitter while the Kaiser Plan Member was still logged-in to the "secure" patient Portal; and

e. On logoff, Kaiser Permanente discloses this action to Adobe, Bing, Google, Quantum Metric, and Twitter.

279. Kaiser Permanente has failed to cure these breaches and continues to disclose to Third Party Wiretappers, Plaintiff's and Breach of Contract Class Members' personally identifiable data and communications with Kaiser Permanente.

Plaintiff and Breach of Contract Class Members Were Damaged

280. Defendants' breach caused Plaintiff and Breach of Contract Class Members the following damages, among others:

a. Nominal damages for each breach of contract by Defendants;

b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information that Plaintiff and Breach of Contract Class Members intended to remain private is no longer private;

d. Defendants eroded the essential confidential nature of the provider-patient relationship;

e. Defendants took something of value from Plaintiff and Breach of Contract Class Members and derived a benefit therefrom without Plaintiff's and Breach of Contract Class Members' knowledge or informed consent and without sharing the benefit of such value;

f. Plaintiff and Breach of Contract Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to maintain confidentiality;

g. Defendants' actions diminished the value of Plaintiff and Breach of Contract Class Members' personal information;

h. Defendants' actions violated the property rights that Plaintiff and Breach of Contract Class Member enjoy in their private communications; and

i. Defendants' actions violated the property rights that Plaintiff and Breach of Contract Class Members enjoy in their personally identifiable medical data and communication.

281. Plaintiff and Breach of Contract Class Members also seek attorney's fees and costs on this claim to the extent allowable.

SIXTH CAUSE OF ACTION
Breach of Implied Contract
(On Behalf of the Nationwide Breach of Contract Sub-Class, or Alternatively, On Behalf of the California Breach of Contract Sub-Class)

282. Plaintiff repeats and incorporates all other paragraphs as if fully set forth herein.

283. Plaintiff brings this claim on behalf of himself and the Nationwide Breach of Contract Sub-Class, or alternatively on behalf of the California Breach of Contract Sub-Class.

284. An implied contract was created between Kaiser Permanente, on the one side, and Plaintiff and Breach of Contract Class Members, on the other hand, whereby Kaiser Permanente offered to provide Plaintiff and Breach of Contract Class Members what it represented to be a secure Portal through which Plaintiff and Breach of Contract Class Members could confidentially make appointments, review medical history, get test results, communicate with providers, and find doctors, among other things, and Plaintiff and Breach of Contract Class Members agreed to use the purportedly secure Portal to make appointments, view medical history, get test results, and find and communicate with doctors, among other things, instead of doing so by other means, such as by phone or in person.

Mutual Assent

285. Such implied contract was created by virtue of the relationship and conduct of the parties, as well as the surrounding circumstances, including, but not limited to:

a. The confidential nature of the medical-provider/patient relationship between Kaiser Permanente and Plaintiff and Breach of Contract Class Members;

b. Kaiser Permanente's express promises, as noted above, to maintain the privacy and confidentiality of patients' personally identifiable data and communications that Plaintiff and Breach of Contract Class Members exchange with Kaiser Permanente at the Site;

c. Kaiser Permanente's creation of a purportedly secure patient Portal that requires a sign-in with a user name and password, which would lead a reasonable person to believe that their communications with Kaiser Permanente while signed in to the Portal would not be shared outside of Kaiser Permanente; and

d. Plaintiff and Breach of Contract Class Members' use of the purportedly secure Portal to make appointments, get test results, and find doctors, among other things, instead of doing so by other means, such as by phone or in person.

286. Kaiser Permanente knew, or had reason to know, that Plaintiff and Breach of Contract Class Members would interpret the parties' relationship and conduct as an agreement to keep Plaintiff and Breach of Contract Class Members' patient status, personally identifiable data, and

communications with Kaiser Permanente inside the Portal confidential when Plaintiff and Breach of Contract Class Members used Kaiser Permanente's patient Portal.

Consideration

287. The patient Portal is not a service Kaiser Permanente provides without receiving anything from Plaintiff and other patients in return. To the contrary, Plaintiff's and Breach of Contract Class Members' use of the Portal confers significant benefit upon Kaiser Permanente—a benefit to which Kaiser Permanente is not entitled—including, but not limited to, increased efficiency, optimized workflow, cost reduction, and receipt of incentive payments from the federal government (United States Department of Health and Human Services) via the Meaningful Use Program.

288. As just one example, patients' use of the patient Portal to access test results and make appointments results in Kaiser Permanente being freed up from performing such tasks of scheduling and reporting on test results for patients, thereby cutting down on long phone calls or in-office communications, increasing efficiency and decreasing costs.

289. As a result, and as further noted above, Kaiser Permanente is able to more efficiently allocate resources and benefits from improved—and, thus, less costly—patient outcomes and increased patient loyalty.

Performance

290. Plaintiff John Doe and Breach of Contract -Class Members performed under the implied contract.

Kaiser Permanente's Breach of the Implied Contract

291. Kaiser Permanente materially breached its implied contract with Plaintiff and Breach of Contract Class Members, by disclosing to third-party companies, Plaintiff and Breach of Contract Class Members' patient status, personally identifiable data, and confidential communications with Kaiser Permanente made within the patient Portal, thereby failing to provide Plaintiff and Class Members with the secure site it agreed to provide.

292. The patient health information Kaiser Permanente used and disclosed to unauthorized third parties for marketing includes:

a. Breach of Contract Class Members' IP addresses, User-Agent data, persistent cookie

identifiers, device identifiers, and/or browser fingerprint information—all of which constitute personally identifiable data both alone and in combination with other data;

b. the date and time of Breach of Contract Class Members' registration for the Portal;

c. the date and time of every Breach of Contract Class Member's sign-in and logoff of the "secure" Portal;

d. the contents of communications Breach of Contract Class Members exchange inside the "secure" Portal;

e. the contents of communications Breach of Contract Class Members exchange after they have logged off the Portal;

f. the contents of communications Breach of Contract Class Members exchange with Kaiser Permanente seeking providers who accept specific insurance products while still signed in to the "secure" Portal; and

g. all other HTTPS communications patients exchange with Kaiser Permanente at the Site that Kaiser Permanente has permitted the third parties to correlate with the Breach of Contract Class Members' status as a patient and the particular dates and times for which they access the "secure" Portal

293. The patient data Kaiser Permanente discloses (Plaintiff and Breach of Contract Class Members patient status, personally identifiable data, and confidential communications with Kaiser Permanente and its providers) is not aggregated as specified in the Privacy Statement.

294. Nevertheless, information that Plaintiff and Breach of Contract Class Members reasonably thought was being transmitted "securely" to Kaiser Permanente within the patient Portal was being disclosed by Kaiser Permanente to unauthorized third parties as follows:

a. A patient signs in to the "secure" patient Portal;

b. On sign-in, Kaiser Permanente discloses the fact of the sign in to Adobe, Bing, Google, Quantum Metric, and Twitter;

c. Once signed-in, if a patient clicked to, for example:

d. view tests, a disclosure of that action was made to Adobe, Bing, Google, Quantum

Metric, and Twitter of the specific tests; or,

e. Find-A-Doctor, or set an appointment, a disclosure of that action was made to Adobe, Bing, Google, Quantum Metric, and Twitter.

f. The above examples of patient communications about the doctor or the appointment was shared with Adobe, Bing, Google, Quantum Metric, and Twitter while the patient was still logged-in to the "secure" patient Portal; and

g. On logoff, Kaiser Permanente discloses this action to Adobe, Bing, Google, Quantum Metric, and Twitter.

295. Kaiser Permanente has failed and refused to cure these breaches and continues to disclose to unauthorized third parties, Plaintiff and Breach of Contract Class Members' patient status, personally identifiable data, and communications with Kaiser Permanente and its providers exchanged on the Site, including the Portal.

Plaintiff and Breach of Contract Class Members Were Damaged

296. Defendants' breach caused Plaintiff and Breach of Contract Class Members the following damages, among others:

a. Nominal damages for each breach of contract by Defendants;

b. General damages for invasion of their rights in an amount to be determined by a jury without reference to specific pecuniary harm;

c. Sensitive and confidential information that Plaintiff and Breach of Contract Class Members intended to remain private is no longer private;

d. Defendants eroded the essential confidential nature of the provider-patient relationship;

e. Defendants took something of value from Plaintiff and Breach of Contract Class Members and derived benefit therefrom without Plaintiff's and Breach of Contract Class Members' knowledge· or informed consent and without sharing the benefit of such value;

f. Plaintiff and Breach of Contract Class Members did not get the full value of the medical services for which they paid, which included Defendants' duty to

maintain confidentiality;

g. Defendants' actions diminished the value of Plaintiff and Breach of Contract Class Members' personal information;

h. Defendants' actions violated the property rights Plaintiff and Breach of Contract Class Members enjoy in their private communications; and

i. Defendants' actions violated the property rights Plaintiff and Breach of Contract Class Members enjoy in their personally identifiable medical data and communication.

297. Plaintiff and Breach of Contract Class Members also seek attorney's fee and costs on this claim to the extent allowable.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff, individually and on behalf of the proposed Classes, respectfully requests that the Court enter an order:

A. Certifying this case as a class action on behalf of the Classes defined above, appointing Plaintiff as the representative of the Classes, and appointing Plaintiff's counsel as the Class Counsel for the Classes;

B. Declaring that Defendants' conduct, as set forth above, violates the laws cited herein;

C. Awarding damages, including nominal, statutory, and punitive damages where applicable, to Plaintiff and the Classes in an amount to be determined at trial;

D. Awarding Plaintiff and the Classes their reasonable litigation expenses, costs and attorneys' fees;

E. Awarding Plaintiff and the Classes pre- and post-judgment interest, to the extent allowable;

F. Awarding such other further injunctive and declaratory relief as is necessary to protect the interests of Plaintiff and the Classes; and

G. Awarding such other and further relief as the Court deems reasonable and just.

IX. DEMAND FOR JURY TRIAL

Pursuant to Rule 38(b) of the Federal Rules of Civil Procedure, Plaintiff demands a jury trial as to all issues triable by a jury.

DATED: May 5, 2023

Respectfully submitted,

KESSLER TOPAZ MELTZER & CHECK, LLP

/s/ Jennifer L. Joost
Jennifer L. Joost (Bar No. 296164)
jjoost@ktmc.com
One Sansome Street, Suite 1850
San Francisco, CA 94104
Telephone: (415) 400-3000
Facsimile: (415) 400-3001

-and-

KESSLER TOPAZ MELTZER & CHECK, LLP
Joseph H. Meltzer
jmeltzer@ktmc.com
Melissa L. Yeates
myeates@ktmc.com
Tyler S. Graden
tgraden@ktmc.com
Jordan E. Jacobson
jjacobson@ktmc.com
280 King of Prussia Road
Radnor, PA 19087
Telephone: (610) 667-7706
Facsimile: (610) 667-7056

Counsel for Plaintiff and the proposed Classes